

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年10月18日 (18.10.2001)

PCT

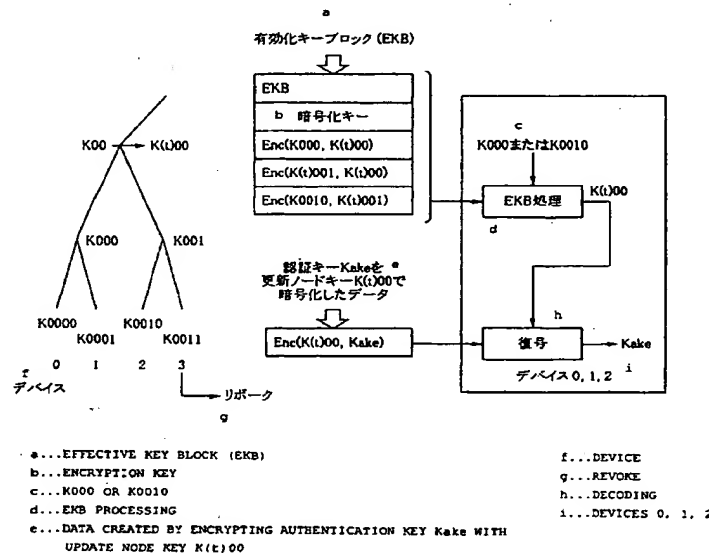
(10) 国際公開番号
WO 01/78298 A1

- (51) 国際特許分類: H04L 9/00, G06F 17/60, G11B 20/10, 20/12
- (21) 国際出願番号: PCT/JP01/02866
- (22) 国際出願日: 2001年4月2日 (02.04.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2000-105329 2000年4月6日 (06.04.2000) JP
特願2000-179695 2000年6月15日 (15.06.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者: および
- (75) 発明者/出願人 (米国についてのみ): 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 大石丈於 (OISHI, Tateo) [JP/JP]. 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
- (81) 指定国 (国内): AU, CN, ID, IN, KR, MX, NO, SG, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: INFORMATION PROCESSING SYSTEM AND METHOD

(54) 発明の名称: 情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体



(57) Abstract: A content key, an authentication key, program data along with an effective key block (EKB) are transmitted by an encryption key structure of a tree structure. The EKB has a structure in which a device constituting a tree leaf holds a leaf key and a limited node key. A specific effective key block (EKB) is generated and distributed to a group specified by a specific node, thus limiting an updateable device. A device not belonging to a group cannot be decoded, ensuring the distribution security of the key and so forth. Keys or data is distributed by an encryption key structure of tree structure, thereby providing an information processing system and method capable of efficiently and safely distributing data.

[続葉有]



— 補正書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

ツリー構造の暗号化鍵構成により、コンテンツキー、認証キー、プログラムデータ等を有効化キーブロック（EKB）とともに送信する。EKBは、ツリーのリーフを構成するデバイスにリーフキー及び限定したノードキーを保有させた構成であり、特定のノードにより特定されるグループに特定の有効化キーブロック（EKB）を生成して配布して、更新可能デバイスを限定することができる。グループに属さないデバイスは復号できず、キー等の配信安全性が確保される。すなわち、ツリー（木）構造の暗号化キー構成により各種キー又はデータの配布を実行して、効率的、安全なデータ配信を可能とした情報処理システム及び方法を実現する。

明細書

情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体

技術分野

本発明は、情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体に関し、特に、暗号処理を伴うシステムにおける暗号処理鍵を配信するシステム及び方法に関する。特に、ツリー構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく抑えて、例えばコンテンツキー配信、あるいは各種鍵の更新の際のデータ配信の負荷を軽減し、かつデータの安全性を保持することを可能とする情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

昨今、ゲームプログラム、音声データ、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいはDVD、CD等の流通可能な記憶媒体を介しての流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、ゲーム機器によってデータ受信、あるいは記憶媒体の装着がなされて再生されたり、あるいはPC等に付属する記録再生機器内の記録デバイス、例えばメモリカード、ハードディスク等に格納されて、格納媒体からの新たな再生により利用される。

ビデオゲーム機器、PC等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはDVD、CD等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要なとなる制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、P C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。したがって、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われなようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にD E S（データ暗号標準：Data encryption standard）がある。

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができ

る。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行う。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはR S A (Rivest-Shamir-Adleman) 暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

上記のようなコンテンツ配信システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはDVD、CD等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツキーを正当なユーザにのみ提供する構成が多く採用されている。コンテンツキー自体の不正なコピー等を防ぐためのコンテンツキーを暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツキーを復号してコンテンツキーを使用可能とする構成が提案されている。

正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツキーの配信前に認証処理を実行することによって行う。一般的な認証処理においては、相手の確認を行うとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツキーを暗号化して通信を行う。認証方

式には、共通鍵暗号方式を用いた相互認証と、公開鍵方式を使用した認証方式があるが、共通鍵を使った認証においては、システムワイドで共通な鍵が必要になり、更新処理等の際に不便である。また、公開鍵方式においては、計算負荷が大きくまた必要なメモリ量も大きくなり、各デバイスにこのような処理手段を設けることは望ましい構成とはいえない。

発明の開示

本発明では、上述のようなデータの送信者、受信者間の相互認証処理に頼ることなく、正当なユーザに対してのみ、安全にデータを送信することを可能とする情報処理システム、情報処理方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

本発明に係る情報処理システムは、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムである。個々のデバイスは、複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される暗号化メッセージデータについての復号処理をキーセットを使用して実行する暗号処理手段を有する。暗号化メッセージデータを配信するメッセージデータ配信手段は、階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）を生成するとともに、更新ノードキーによって暗号化したメッセージデータを生成して配信する。

さらに、本発明の情報処理システムの一実施態様において、デバイスにおける暗号処理手段は、有効化キーブロック（EKB）の処理により、更新ノードキーを取得し、取得した更新ノードキーにより暗号化メッセージデータの復号を実行する。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータ

は、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、認証処理において用いられる認証キーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、認証処理において用いられる認証キーである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータは、プログラムコードである。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータ配信手段は、有効化キーブロック（EKB）と、メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと、コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信する構成である。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータ配信手段とデバイスは、それぞれ認証処理を実行する認証処理手段を有する。メッセージデータの配信は、メッセージデータ配信手段とデバイス間での認証処理が成立したことを条件として行われる。

さらに、本発明の情報処理システムの一実施態様において、メッセージデータ配信手段とデバイス間には異なる中間デバイスが介在する。メッセージデータ配信手段は、メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（EKB）と暗号化メッセージデータを生成して配信する。

さらに、本発明の情報処理システムの一実施態様において、階層ツリー構造は、1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループによって構成されるカテゴリグループを含む。カテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたカテゴリに属するデバイスの集合として構成されている。

さらに、本発明の情報処理システムの一実施態様において、カテゴリグループは、さらに階層ツリー構造の下位段に1以上のサブカテゴリを含む。サブカテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたサブカテゴリに属するデバイスの集合として構成されている。

本発明に係る情報処理方法は、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータをメッセージデータ配線手段から配信する情報処理方法であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した有効化キープロック（EKB）を生成するとともに、更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、暗号化メッセージデータについての復号処理をキーセットを使用して実行する復号処理ステップとを有する。

さらに、本発明の情報処理方法の一実施態様において、復号処理ステップは、有効化キープロック（EKB）の処理により、更新ノードキーを取得する更新ノードキー取得ステップと、更新ノードキーにより暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含む。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、認証処理において用いられる認証キーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、認証処理において用いられる認証キーである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータは、プログラムコードである。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータ配信手段は、有効化キーブロック（E K B）と、メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーとコンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信する。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータ配信手段とデバイスは、相互間の認証処理を実行し、メッセージデータの配信は、メッセージデータ配信手段とデバイス間での認証処理が成立したことを条件として配信する。

さらに、本発明の情報処理方法の一実施態様において、メッセージデータ配信手段とデバイス間には異なる中間デバイスが介在する。メッセージデータ配信手段は、メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（E K B）と暗号化メッセージデータを生成して配信する。

本発明に係る情報記録媒体は、データを格納した情報記録媒体であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（E K B）と、更新ノードキーによって暗号化したメッセージデータとを格納している。

さらに、本発明の情報記録媒体の一実施態様において、メッセージデータはコンテンツの復号に用いるコンテンツキーである。情報記録媒体は、さらに、コンテンツキーによって暗号化された暗号化コンテンツを格納している。

さらに、本発明の情報記録媒体の一実施態様において、コンテンツとコンテンツの対応するコンテンツキーを取得するために使用される有効化キーブロック（E K B）を対応付けた対応付けデータを格納している。

さらに、本発明の情報記録媒体の一実施態様において、コンテンツのインテグ

リティ・チェック値（ICV）データを格納している。

本発明に係るプログラム提供媒体は、暗号化コンテンツデータの復号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体である。コンピュータ・プログラムは、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、更新ノードキーをグループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）の復号処理により、更新ノードキーを取得する更新ノードキー取得ステップと、更新ノードキーによる復号処理を実行して、暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するステップと、コンテンツキーにより暗号化コンテンツの復号を実行するステップとを含む。

本発明では、ツリー（木）構造の階層的構造の暗号化鍵配信構成を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの暗号鍵であるコンテンツキー若しくは認証処理に用いる認証キー、あるいはプログラムコード等を有効化キーブロックとともに配信する構成としている。このようにすることにより、正当なデバイスのみが復号可能なデータを安全に配信することが可能となる。

なお、本発明に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、

本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

図 1 は、本発明の情報処理システムの構成例を説明する図である。

図 2 は、本発明の情報処理システムにおいて適用可能な記録再生装置の構成例を示すブロック図である。

図 3 は、本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

図 4 A 及び図 4 B は、本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キーブロック (EKB) の例を示す図である。

図 5 は、本発明の情報処理システムにおけるコンテンツキーの有効化キーブロック (EKB) を使用した配布例と復号処理例を示す図である。

図 6 は、本発明の情報処理システムにおける有効化キーブロック (EKB) のフォーマット例を示す図である。

図 7 A 乃至図 7 C は、本発明の情報処理システムにおける有効化キーブロック (EKB) のタグの構成を説明する図である。

図 8 A 及び図 8 B は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

図 9 は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

図 10 は、本発明の情報処理システムにおける有効化キーブロック (EKB) とコンテンツを記録媒体に格納した場合の対応について説明する図である。

図 11 A 及び図 11 B は、本発明の情報処理システムにおける有効化キーブロック (EKB) と、コンテンツキーを送付する処理を従来の送付処理と比較した

図である。

図 1 2 は、本発明の情報処理システムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。

図 1 3 は、本発明の情報処理システムにおける有効化キープブロック (E K B) と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 1) である。

図 1 4 は、本発明の情報処理システムにおける有効化キープブロック (E K B) と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 2) である。

図 1 5 は、本発明の情報処理システムにおいて適用可能な公開鍵暗号方式による認証処理シーケンスを示す図である。

図 1 6 は、本発明の情報処理システムにおいて公開鍵暗号方式による認証処理を用いて有効化キープブロック (E K B) と、コンテンツキーを併せて配信する処理を示す図である。

図 1 7 は、本発明の情報処理システムにおいて有効化キープブロック (E K B) と、暗号化プログラムデータを併せて配信する処理を示す図である。

図 1 8 は、本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値 (I C V) の生成に使用する M A C 値生成例を示す図である。

図 1 9 は、本発明の情報処理システムにおける有効化キープブロック (E K B) と、I C V 生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 1) である。

図 2 0 は、本発明の情報処理システムにおける有効化キープブロック (E K B) と、I C V 生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図 (その 2) である。

図 2 1 A 及び図 2 1 B は、本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値 (I C V) をメディアに格納した場合のコピー防止機能を説明する図である。

図 2 2 は、本発明の情報処理システムにおいて適用可能なコンテンツ・インテ

グリティ・チェック値（ICV）をコンテンツ格納媒体と別に管理する構成を説明する図である。

図23は、本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

発明を実施するための最良の形態

[システム概要]

図1に本発明のデータ処理システムが適用可能なコンテンツ配信システム例を示す。コンテンツの配信側10は、コンテンツ受信側20の有する様々なコンテンツ再生可能な機器に対してコンテンツ、あるいはコンテンツキーを暗号化して送信する。受信側20における機器では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキーを取得して、画像データ、音声データの再生、あるいは各種プログラムの実行等を行う。コンテンツの配信側10とコンテンツ受信側20との間のデータ交換は、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して実行される。

コンテンツの配信側10は例えば所謂サーバとして構成され、ハードディスクドライブなどの情報記憶手段やCPUなどの情報処理装置を有する既存のパーソナルコンピュータで構成される。コンテンツの配信側10は後述するコンテンツプロバイダとして、あるいはサービスプロバイダやアプリケーションプロバイダが同等の機能を有していてもよい。コンテンツの配信側10のデータ配信手段としては、インターネット11、衛星放送12、電話回線13、DVD、CD等のメディア14等があり、一方、コンテンツ受信側20のデバイスとしては、パーソナルコンピュータ（PC）21、ポータブルデバイス（PD）22、携帯電話、PDA（Personal Digital Assistants）等の携帯機器23、DVD、CDプレーヤ等の記録再生器24、ゲーム端末等の再生専用器25等がある。これらコンテンツ受信側20の各デバイスは、コンテンツ配信側10から提供されたコンテンツをネットワーク等の通信手段あるいは、あるいはメディア30から取得する。

[デバイス構成]

図2に、図1に示すコンテンツ受信側20のデバイスの一例として、記録再生装置100の構成ブロック図を示す。記録再生装置100は、入出力I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F (Interface) 140、暗号処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、記録媒体195のドライブ190を有し、これらはバス110によって相互に接続されている。

入出力I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F 140に出力するとともに、入出力I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F 140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F 140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号の暗号化、復号処理、あるいは認証処理を実行し、暗号データ、復号データ等をバス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ROM 160は、記録再生装置によって処理されるプログラムデータを格納す

る。CPU 170は、ROM 160、メモリ 180に記憶されたプログラムを実行することで、MP EGコーデック 130や暗号処理手段 150等を制御する。メモリ 180は、例えば、不揮発性メモリで、CPU 170が実行するプログラムや、CPU 170の動作上必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。ドライブ 190は、デジタルデータを記録再生可能な記録媒体 195を駆動することにより、記録媒体 195からデジタルデータを読み出し（再生し）、バス 110上に出力するとともに、バス 110を介して供給されるデジタルデータを、記録媒体 195に供給して記録させる。

記録媒体 195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ 190に対して着脱可能な構成であるとする。ただし、記録媒体 195は、記録再生装置 100に内蔵する構成としてもよい。

なお、図2に示す暗号処理手段 150は、1つのワンチップLSIとして構成してもよく、また、ソフトウェア、ハードウェアを組み合わせた構成によって実現する構成としてもよい。

[キー配信構成としてのツリー（木）構造について]

次に、図1に示すコンテンツ配信側 10からコンテンツ受信側 20の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵の保有構成及びデータ配信構成を図3を用いて説明する。

図3の最下段に示すナンバ0～15がコンテンツ受信側 20の個々のデバイスである。すなわち図3に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図3に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーからなるキーセットをメモリに格納する。図3の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKR

(ルートキー) から、最下段から 2 番目の節 (ノード) に記載されたキー: KR ~ K 1 1 1 をノードキーとする。

図 3 に示すツリー構成において、例えばデバイス 0 はリーフキー K 0 0 0 0 と、ノードキー: K 0 0 0、K 0 0、K 0、KR を所有する。デバイス 5 は K 0 1 0 1、K 0 1 0、K 0 1、K 0、KR を所有する。デバイス 15 は、K 1 1 1 1、K 1 1 1、K 1 1、K 1、KR を所有する。なお、図 3 のツリーにはデバイスが 0 ~ 15 の 16 個のみ記載され、ツリー構造も 4 段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図 3 のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成された DVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図 3 に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図 3 の点線で囲んだ部分、すなわちデバイス 0、1、2、3 を同一の記録媒体を用いる 1 つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、図 3 の点線で囲んだ部分、すなわちデバイス 0、1、2、3 を 1 つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図 3 のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、メッセージデータ配信手段として機能する。

なお、ノードキー、リーフキーは、ある 1 つの鍵管理センタによって統括して

管理してもよいし、各グループに対する様々なデータ送受信を行うプロバイダ、決済機関等のメッセージデータ配信手段によってグループ毎に管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図3から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス0, 1, 2, 3のみに提供することが可能となる。例えば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc(K00, Kcon)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcon)を解いてコンテンツキー: Kconを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

また、ある時点tにおいて、デバイス3の所有する鍵: K0011, K001, K00, K0, KRが攻撃者(ハッカー)により解析されて露呈したことが発覚した場合、それ以降、システム(デバイス0, 1, 2, 3のグループ)で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代(Generation): tの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図4Aに示す有効化キーブロック(EKB: Enabling Key Block)と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納し

てデバイス0, 1, 2に供給することによって実行される。なお、有効化キーブロック (EKB) は、図3に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック (EKB) は、キー更新ブロック (KRB : Key Renewal Block) と呼ばれることもある。

図4Aに示す有効化キーブロック (EKB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4の例は、図3に示すツリー構造中のデバイス0, 1, 2において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図3から明らかなように、デバイス0, デバイス1は、更新ノードキーとして $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

図4AのEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図4Aの下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図4Aの上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4Aの上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス $K0000$ 、 $K0001$ は、図4Aの上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し、 $K(t)00$ を取得し、以下、図4Aの上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4Aの上から1段目の暗号化キー

$Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 $K(t)R$ を得ることができる。なお、図 4 A のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図 3 に示すツリー構造の上位段のノードキー： $K(t)0, K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図 4 B の有効化キーブロック (EKB) を用いることで、更新ノードキー $K(t)00$ をデバイス 0, 1, 2 に配布することができる。

図 4 B に示す EKB は、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図 3 に点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のコンテンツキー $K(t)con$ が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たな共通の更新コンテンツキー： $K(t)con$ を暗号化したデータ $Enc(K(t), K(t)con)$ を図 4 B に示す EKB とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス 0, 1, 2 は EKB を処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 t 時点でのコンテンツキー $K(t)con$ を得ることが可能になる。

[EKB を使用したコンテンツキーの配布]

図 5 に、 t 時点でのコンテンツキー $K(t)con$ を得る処理例として、 $K(t)00$ を用いて新たな共通のコンテンツキー $K(t)con$ を暗号化したデータ $Enc(K(t)00, K(t)con)$ と図 4 B に示す EKB とを記録媒体を介して受領したデバイス 0 の処理を示す。すなわち EKB による暗号化メッセージデータをコンテンツキー $K(t)con$ とした例である。

図 5 に示すように、デバイス 0 は、記録媒体に格納されている世代： t 時点の EKB と自分が予め格納しているノードキー $K000$ を用いて上述したと同様の EKB 処理により、ノードキー $K(t)00$ を生成する。さらに、復号した更新

ノードキー $K(t)00$ を用いて更新コンテンツキー $K(t)con$ を復号して、後にそれを使用するために自分だけが持つリーフキー $K0000$ で暗号化して格納する。

[EKBのフォーマット]

図6に有効化キーブロック(EKB)のフォーマット例を示す。バージョン601は、有効化キーブロック(EKB)のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デブスは、有効化キーブロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポイント603は、有効化キーブロック(EKB)中のデータ部の位置を示すポイントであり、タグポイント604はタグ部の位置、署名ポイント605は署名の位置を示すポイントである。

データ部606は、例えば更新するノードキーを暗号化したデータを格納する。例えば図5に示すような更新されたノードキーに関する各暗号化キー等を格納する。

タグ部607は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図7A乃至図7Cを用いて説明する。図7A乃至図7Cでは、データとして先に図4Aで説明した有効化キーブロック(EKB)を送付する例を示している。この時のデータは、図7Bに示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図7Aに示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、全てのデータにタグが設定され、図7Cに示すデータ列、及びタグ列が構成される。

タグは、データ $Enc(K_{xxx}, K_{yyy})$ がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータ $Enc(K_{xxx}, K_{yyy}) \dots$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図4で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : $Enc(K(t)_0, K(t)_{root})$

00 : $Enc(K(t)_{00}, K(t)_0)$

000 : $Enc(K((t)_{000}, K(t)_{00}))$

... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

図6に戻って、EKBフォーマットについてさらに説明する。署名 (Signature) は、有効化キーブロック (EKB) を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック (EKB) 発行者が発行した有効化キーブロック (EKB) であることを確認する。

[EKBを使用したコンテンツキー及びコンテンツの配信]

上述の例では、コンテンツキーのみをEKBとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、EKBによって暗号化したコンテンツキー暗号鍵を併せて送付する構成について以下説明する。

図8A及び図8Bにこのデータ構成を示す。図8Aに示す構成において、 $Enc(K_{con}, content)_{801}$ は、コンテンツ (Content) をコンテンツキー (K_{con}) で暗号化したデータであり、 $Enc(KEK, K_{con})_{802}$ は、コンテンツキー (K_{con}) をコンテンツキー暗号キー ($KEK : Key En$

encryption Key) で暗号化したデータであり、 $\text{Enc}(\text{EKB}, \text{KEK}) 803$ は、コンテンツキー暗号キー KEK を有効化キーブロック (EKB) によって暗号化したデータであることを示す。

ここで、コンテンツキー暗号キー KEK は、図 3 で示すノードキー ($\text{K}000$, $\text{K}00\dots$)、あるいはルートキー (KR) 自体であってもよく、またノードキー ($\text{K}000$, $\text{K}00\dots$)、あるいはルートキー (KR) によって暗号化されたキーであってもよい。

図 8 B は、複数のコンテンツがメディアに記録され、それぞれが同じ $\text{Enc}(\text{EKB}, \text{KEK}) 805$ を利用している場合の構成例を示す、このような構成においては、各データに同じ $\text{Enc}(\text{EKB}, \text{KEK})$ を付加することなく、 $\text{Enc}(\text{EKB}, \text{KEK})$ にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

図 9 にコンテンツキー暗号キー KEK を、図 3 に示すノードキー $\text{K}00$ を更新した更新ノードキー $\text{K}(t)00$ として構成した場合の例を示す。この場合、図 3 の点線枠で囲んだグループにおいてデバイス 3 が、例えば鍵の漏洩によりリボーク (排除) されているとして、他のグループのメンバ、すなわち、デバイス 0, 1, 2 に対して図 9 に示す有効化キーブロック (EKB) と、コンテンツキー (Kcon) をコンテンツキー暗号キー ($\text{KEK} = \text{K}(t)00$) で暗号化したデータと、コンテンツ (content) をコンテンツキー (Kcon) で暗号化したデータとを配信することにより、デバイス 0, 1, 2 はコンテンツを得ることができる。

図 9 の右側には、デバイス 0 における復号手順を示してある。デバイス 0 は、まず、受領した有効化キーブロックから自身の保有するリーフキー $\text{K}000$ を用いた復号処理により、コンテンツキー暗号キー ($\text{KEK} = \text{K}(t)00$) を取得する。次に、 $\text{K}(t)00$ による復号によりコンテンツキー Kcon を取得し、さらにコンテンツキー Kcon によりコンテンツの復号を行う。これらの処理により、デバイス 0 はコンテンツを利用可能となる。デバイス 1, 2 においても各々異なる処理手順で EKB を処理することにより、コンテンツキー暗号キー ($\text{KEK} = \text{K}(t)00$) を取得することが可能となり、同様にコンテンツを利用す

ることが可能となる。

図3に示す他のグループのデバイス4, 5, 6…は、この同様のデータ(EKB)を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー($K_{EK} = K(t)00$)を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー($K_{EK} = K(t)00$)を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

このように、EKBを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

なお、有効化キーブロック(EKB)、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック(EKB)、コンテンツキー、暗号化コンテンツをDVD、CD等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック(EKB)の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

図10に記録媒体に暗号化コンテンツとともに有効化キーブロック(EKB)を格納した構成例を示す。図10に示す例においては、記録媒体にコンテンツC1～C4が格納され、さらに各格納コンテンツに対応する有効化キーブロック(EKB)を対応付けたデータが格納され、さらにバージョンMの有効化キーブロック(EKB_M)が格納されている。例えば EKB_1 はコンテンツC1を暗号化したコンテンツキー K_{cn1} を生成するのに使用され、例えば EKB_2 はコンテンツC2を暗号化したコンテンツキー K_{cn2} を生成するのに使用される。この例では、バージョンMの有効化キーブロック(EKB_M)が記録媒体に格納されており、コンテンツC3, C4は有効化キーブロック($EKB_$

M)に対応付けられているので、有効化キーブロック(EKB__M)の復号によりコンテンツC3, C4のコンテンツキーを取得することができる。EKB__1、EKB__2はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なEKB__1, EKB__2を取得することが必要となる。

図11A及び図11Bに、複数のデバイス間でコンテンツキーが流通する場合のEKBを利用したコンテンツキーの配信と、従来のコンテンツキー配信処理の比較例を示す。図11Aが従来構成であり、図11Bが本発明の有効化キーブロック(EKB)を利用した例である。なお、図11A及び図11BにおいてKa(Kb)は、KbをKaで暗号化したデータであることを示す。

図11Aに示すように、従来は、データ送受信者の正当性を確認し、またデータ送信の暗号化処理に使用するセッションキーKsesを共有するために各デバイス間において、認証処理及び鍵交換処理(AKE: Authentication and Key Exchange)を実行し、認証が成立したことを条件としてセッションキーKsesでコンテンツキーKconを暗号化して送信する処理を行っていた。

例えば図11AのPCにおいては、受信したセッションキーで暗号化したコンテンツキーKses(Kcon)をセッションキーで復号してKconを得ることが可能であり、さらに取得したKconをPC自体の保有する保存キーKstrで暗号化して自身のメモリに保存することが可能となる。

図11Aにおいて、コンテンツプロバイダは、図11Aの記録デバイス1101にのみデータを利用可能な形で配信したい場合でも、間にPC、再生装置が存在する場合は、図11Aに示すように認証処理を実行し、それぞれのセッションキーでコンテンツキーを暗号化して配信するといった処理が必要となる。また、間に介在するPC、再生装置においても認証処理において生成し共有することになったセッションキーを用いることで暗号化コンテンツキーを復号してコンテンツキーを取得可能となる。

一方、図11Bに示す有効化キーブロック(EKB)を利用した例においては、コンテンツプロバイダから有効化キーブロック(EKB)と、有効化キーブロック(EKB)の処理によって得られるノードキー、又はルートキーによってコン

テンツキーK c o nを暗号化したデータ（図の例ではK r o o t (K c o n)）を配信することにより、配信したE K Bの処理が可能な機器においてのみコンテンツキーK c o nを復号して取得することが可能になる。

したがって、例えば図11Bの右端にのみ利用可能な有効化キーブロック（E K B）を生成して、その有効化キーブロック（E K B）と、そのE K B処理によって得られるノードキー、又はルートキーによってコンテンツキーK c o nを暗号化したデータを併せて送ることにより、間に存在するP C、再生機器等は、自身の有するリーフキー、ノードキーによっては、E K Bの処理を実行することができない。したがって、データ送受信デバイス間での認証処理、セッションキーの生成、セッションキーによるコンテンツキーK c o nの暗号化処理といった処理を実行することなく、安全に正当なデバイスに対してのみ利用可能なコンテンツキーを配信することが可能となる。

P C、記録再生器にも利用可能なコンテンツキーを配信したい場合は、それぞれにおいて処理可能な有効化キーブロック（E K B）を生成して、配信することにより、共通のコンテンツキーを取得することが可能となる。

〔有効化キーブロック（E K B）を使用した認証キーの配信（共通鍵方式）〕

上述の有効化キーブロック（E K B）を使用したデータあるいはキーの配信において、デバイス間で転送される有効化キーブロック（E K B）及びコンテンツあるいはコンテンツキーは常に同じ暗号化形態を維持しているため、データ伝走路を盗み出して記録し、再度、後で転送する、いわゆるリプレイアタックにより、不正コピーが生成される可能性がある。これを防ぐ構成としては、データ転送デバイス間において、従来と同様の認証処理及び鍵交換処理を実行することが有効な手段である。ここでは、この認証処理及び鍵交換処理を実行する際に使用する認証キーK a k eを上述の有効化キーブロック（E K B）を使用してデバイスに配信することにより、安全な秘密鍵として共有する認証キーを持ち、共通鍵方式に従った認証処理を実行する構成について説明する。すなわちE K Bによる暗号化メッセージデータを認証キーとした例である。

図12に、共通鍵暗号方式を用いた相互認証方法（ISO/IEC 9798-2）を示す。

図12においては、共通鍵暗号方式としてDESを用いているが、共通鍵暗号方式であれば他の方式も可能である。図12において、まず、Bが64ビットの乱数Rbを生成し、Rb及び自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Kabを用いてデータを暗号化し、Bに返送する。なお、鍵Kabは、A及びBに共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。DESのCBCモードを用いた鍵Kabによる暗号化処理は、例えばDESを用いた処理においては、初期値とRaの排他的論理和を求め、DES暗号化部において、鍵Kabを用いて暗号化し、暗号文E1を生成し、続けて暗号文E1とRbの排他的論理和を求め、DES暗号化部において、鍵Kabを用いて暗号化し、暗号文E2を生成し、さらに、暗号文E2とID(b)の排他的論理和を求め、DES暗号化部において、鍵Kabを用いて暗号化して生成した暗号文E3とによって送信データ(Token-AB)を生成する。

これを受信したBは、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵Kab(認証キー)で復号化する。受信データの復号化方法は、まず、暗号文E1を認証キーKabで復号化し、乱数Raを得る。次に、暗号文E2を認証キーKabで復号化し、その結果とE1の排他的論理和を求め、Rbを得る。最後に、暗号文E3を認証キーKabで復号化し、その結果とE2の排他的論理和を求め、ID(b)を得る。こうして得られたRa、Rb、ID(b)のうち、Rb及びID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

次にBは、認証後に使用するセッションキー(Kses)を生成する(生成方法は、乱数を用いる)。そして、Rb、Ra、Ksesの順に、DESのCBCモードで認証キーKabを用いて暗号化し、Aに返送する。

これを受信したAは、受信データを認証キーKabで復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたRb、Ra、Ksesの内、Rb及びRaが、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッションキーKsesは、認証後の秘

密通信のための共通鍵として利用される。

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

上述の認証処理においては、A、Bは共通の認証キー K_{ab} を共有する。この共通鍵 K_{ab} を上述の有効化キープロック (EKB) を使用してデバイスに配信する。

例えば、図12の例では、A、又はBのいずれかが他方が復号可能な有効化キープロック (EKB) を生成して生成した有効化キープロック (EKB) によって認証キー K_{ab} を暗号化して、他方に送信する構成としてもよいし、あるいは第3者がデバイスA、Bに対して双方が利用可能な有効化キープロック (EKB) を生成してデバイスA、Bに対して生成した有効化キープロック (EKB) によって認証キー K_{ab} を暗号化して配信する構成としてもよい。

図13及び図14に複数のデバイスに共通の認証キー K_{ake} を有効化キープロック (EKB) によって配信する構成例を示す。図13はデバイス0, 1, 2, 3に対して復号可能な認証キー K_{ake} を配信する例、図14はデバイス0, 1, 2, 3中のデバイス3をリボーク (排除) してデバイス0, 1, 2に対してのみ復号可能な認証キーを配信する例を示す。

図13の例では、更新ノードキー $K(t)_{00}$ によって、認証キー K_{ake} を暗号化したデータとともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)_{00}$ を復号可能な有効化キープロック (EKB) を生成して配信する。それぞれのデバイスは、図13の右側に示すようにまず、EKBを処理 (復号) することにより、更新されたノードキー $K(t)_{00}$ を取得し、次に、取得したノードキー $K(t)_{00}$ を用いて暗号化された認証キー： $Enc(K(t)_{00}, K_{ake})$ を復号して認証キー K_{ake} を得ることが可能となる。

その他のデバイス4, 5, 6, 7…は同一の有効化キープロック (EKB) を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキー $K(t)_{00}$ を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

一方、図14の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2に対してのみ復号可能な有効化キープロック（EKB）を生成して配信した例である。図14に示す有効化キープロック（EKB）と、認証キー（Kake）をノードキー（K(t)00）で暗号化したデータを配信する。

図14の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受領した有効化キープロックから自身の保有するリーフキー又はノードキーを用いた復号処理により、更新ノードキー（K(t)00）を取得する。次に、K(t)00による復号により認証キーKakeを取得する。

図3に示す他のグループのデバイス4, 5, 6…は、この同様のデータ（EKB）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（K(t)00）を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（K(t)00）を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

このように、EKBを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。

〔公開鍵認証と有効化キープロック（EKB）を使用したコンテンツキーの配信〕

次に、公開鍵認証と有効化キープロック（EKB）を使用したコンテンツキーの配信処理について説明する。まず、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数Rbを生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数Ra及び素数pより小さい乱数Akを生成する。そして、ベースポイントGをAk倍した点Av=Ak×Gを求め、Ra、Rb、Av（X

座標とY座標)に対する電子署名A. Sigを生成し、Aの公開鍵証明書とともにBに返送する。ここで、Ra及びRbはそれぞれ64ビット、AvのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。

Aの公開鍵証明書、Ra、Rb、Av、電子署名A. Sigを受信したBは、Aが送信してきたRbが、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名A. Sigを検証する。

次に、Bは、素数pより小さい乱数Bkを生成する。そして、ベースポイントGをBk倍した点Bv = $Bk \times G$ を求め、Rb、Ra、Bv (X座標とY座標)に対する電子署名B. Sigを生成し、Bの公開鍵証明書とともにAに返送する。

Bの公開鍵証明書、Rb、Ra、Av、電子署名B. Sigを受信したAは、Bが送信してきたRaが、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名B. Sigを検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

両者が認証に成功した場合には、Bは $Bk \times Av$ (Bkは乱数だが、Avは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要)を計算し、Aは $Ak \times Bv$ を計算し、これら点のX座標の下位64ビットをセッションキーとして以降の通信に使用する (共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合)。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッションキーで暗号化されるだけでなく、電子署名も付されることがある。

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

図16に公開鍵認証と有効化キーブロック(EKB)を使用したコンテンツキーの配信処理例を示す。まずコンテンツプロバイダとPC間において図15で説

明した公開鍵方式による認証処理が実行される。コンテンツプロバイダは、コンテンツキー配信先である再生装置、記録媒体の有するノードキー、リーフキーによって復号可能なEKBを生成して、更新ノードキーによる暗号化を実行したコンテンツキーE (Kcon) と、有効化キーブロック (EKB) とをPC間の認証処理において生成したセッションキーKsesで暗号化してPCに送信する。

PCはセッションキーで暗号化された[更新ノードキーによる暗号化を実行したコンテンツキーE (Kcon) と、有効化キーブロック (EKB)]をセッションキーで復号した後、再生装置、記録媒体に送信する。

再生装置、記録媒体は、自身の保有するノードキー又はリーフキーによって[更新ノードキーによる暗号化を実行したコンテンツキーE (Kcon) と、有効化キーブロック (EKB)]を復号することによってコンテンツキーKconを取得する。

この構成によれば、コンテンツプロバイダとPC間での認証を条件として[更新ノードキーによる暗号化を実行したコンテンツキーE (Kcon) と、有効化キーブロック (EKB)]が送信されるので、例えば、ノードキーの漏洩があった場合でも、確実な相手に対するデータ送信が可能となる。

[プログラムコードの有効化キーブロック (EKB) を使用した配信]

上述した例では、コンテンツキー、認証キー等を有効化キーブロック (EKB) を用いて暗号化して配信する方法を説明したが、様々なプログラムコードを有効化キーブロック (EKB) を用いて配信する構成も可能である。すなわちEKBによる暗号化メッセージデータをプログラムコードとした例である。以下、この構成について説明する。

図17にプログラムコードを有効化キーブロック (EKB) の例えば更新ノードキーによって暗号化してデバイス間で送信する例を示す。デバイス1701は、デバイス1702の有するノードキー、リーフキーによって復号可能な有効化キーブロック (EKB) と、有効化キーブロック (EKB) に含まれる更新ノードキーで暗号処理したプログラムコードをデバイス1702に送信する。デバイス1702は受信したEKBを処理して更新ノードキーを取得して、さらに取得した更新ノードキーによってプログラムコードの復号を実行して、プログラムコー

ドを得る。

図17に示す例では、さらに、デバイス1702において取得したプログラムコードによる処理を実行して、その結果をデバイス1701に返して、デバイス1701がその結果に基づいて、さらに処理を続行する例を示している。

このように有効化キープロック (EKB) と、有効化キープロック (EKB) に含まれる更新ノードキーで暗号処理したプログラムコードを配信することにより、特定のデバイスにおいて解読可能なプログラムコードを前述の図3で示した特定のデバイス、あるいはグループに対して配信することが可能となる。

[送信コンテンツに対するチェック値 (ICV: Integrity Check Value) を対応させる構成]

次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値 (ICV) を生成して、コンテンツに対応付けて、ICVの計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

コンテンツのインテグリティ・チェック値 (ICV) は、例えばコンテンツに対するハッシュ関数を用いて計算され、 $ICV = hash(K_{icv}, C1, C2, \dots)$ によって計算される。K_{icv}はICV生成キーである。C1, C2はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号 (MAC: Message Authentication Code) が使用される。

DES暗号処理構成を用いたMAC値生成例を図18に示す。図18の構成に示すように対象となるメッセージを8バイト単位に分割し、(以下、分割されたメッセージをM1、M2、...、MNとする)、まず、初期値 (Initial Value (以下、IVとする)) とM1の排他的論理和を求める (その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵 (以下、K1とする) を用いて暗号化する (出力をE1とする)。続けて、E1とM2の排他的論理和を求め、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する (出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号 (MAC (Message Authentication Code)) となる。

このようなコンテンツのMAC値とICV生成キーにハッシュ関数を適用して

用いてコンテンツのインテグリティ・チェック値 (ICV) が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成した ICV と、新たにコンテンツに基づいて生成した ICV とを比較して同一の ICV が得られればコンテンツに改竄のないことが保証され、ICV が異なれば、改竄があったと判定される。

[チェック値 (ICV) の生成キー K_{icv} を EKB によって配布する構成]

次に、コンテンツのインテグリティ・チェック値 (ICV) 生成キーである K_{icv} を上述の有効化キーブロックによって送付する構成について説明する。すなわち EKB による暗号化メッセージデータをコンテンツのインテグリティ・チェック値 (ICV) 生成キーとした例である。

図 19 及び図 20 に複数のデバイスに共通のコンテンツを送付した場合、それらのコンテンツの改竄の有無を検証するためのインテグリティ・チェック値生成キー K_{icv} を有効化キーブロック (EKB) によって配信する構成例を示す。図 19 はデバイス 0, 1, 2, 3 に対して復号可能なチェック値生成キー K_{icv} を配信する例、図 20 はデバイス 0, 1, 2, 3 中のデバイス 3 をリポーク (排除) してデバイス 0, 1, 2 に対してのみ復号可能なチェック値生成キー K_{icv} を配信する例を示す。

図 19 の例では、更新ノードキー $K(t)_{00}$ によって、チェック値生成キー K_{icv} を暗号化したデータとともに、デバイス 0, 1, 2, 3 においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)_{00}$ を復号可能な有効化キーブロック (EKB) を生成して配信する。それぞれのデバイスは、図 19 の右側に示すようにまず、EKB を処理 (復号) することにより、更新されたノードキー $K(t)_{00}$ を取得し、次に、取得したノードキー $K(t)_{00}$ を用いて暗号化されたチェック値生成キー: $Enc(K(t)_{00}, K_{icv})$ を復号してチェック値生成キー K_{icv} を得ることが可能となる。

その他のデバイス 4, 5, 6, 7... は同一の有効化キーブロック (EKB) を受信しても自身の保有するノードキー、リーフキーでは、EKB を処理して更新されたノードキー $K(t)_{00}$ を取得することができないので、安全に正当なデ

バイスに対してのみチェック値生成キーを送付することができる。

一方、図20の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2に対してのみ復号可能な有効化キープロック（EKB）を生成して配信した例である。図20に示す有効化キープロック（EKB）と、チェック値生成キー（Kicv）をノードキー（K(t)00）で暗号化したデータを配信する。

図20の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受領した有効化キープロックから自身の保有するリーフキー又はノードキーを用いた復号処理により、更新ノードキー（K(t)00）を取得する。次に、K(t)00による復号によりチェック値生成キーKicvを取得する。

図3に示す他のグループのデバイス4, 5, 6…は、この同様のデータ（EKB）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（K(t)00）を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（K(t)00）を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

このように、EKBを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

このようなコンテンツのインテグリティ・チェック値（ICV）を用いることにより、EKBと暗号化コンテンツの不正コピーを排除することができる。例えば図21A及び図21Bに示すように、コンテンツC1とコンテンツC2とをそれぞれのコンテンツキーを取得可能な有効化キープロック（EKB）とともに格納したメディア1があり、これをそのままメディア2にコピーした場合を想定する。EKBと暗号化コンテンツのコピーは可能であり、これをEKBを復号可能なデバイスでは利用できることになる。

図21Bに示すように各メディアに正当に格納されたコンテンツに対応付けてインテグリティ・チェック値（ICV(C1, C2)）を格納する構成とする。

なお、 $(ICV(C1, C2))$ は、コンテンツ $C1$ とコンテンツ $C2$ にハッシュ関数を用いて計算されるコンテンツのインテグリティ・チェック値である $ICV = hash(Kicv, C1, C2)$ を示している。図 21B の構成において、メディア 1 には正当にコンテンツ 1 とコンテンツ 2 が格納され、コンテンツ $C1$ とコンテンツ $C2$ に基づいて生成されたインテグリティ・チェック値 $(ICV(C1, C2))$ が格納される。また、メディア 2 には正当にコンテンツ 1 が格納され、コンテンツ $C1$ に基づいて生成されたインテグリティ・チェック値 $(ICV(C1))$ が格納される。この構成において、メディア 1 に格納された $\{EKB, \text{コンテンツ 2}\}$ をメディア 2 にコピーしたとすると、メディア 2 で、コンテンツチェック値を新たに生成すると $ICV(C1, C2)$ が生成されることになり、メディアに格納されている $Kicv(C1)$ と異なり、コンテンツの改竄あるいは不正なコピーによる新たなコンテンツの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップに ICV チェックを実行して、生成 ICV と格納 ICV の一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのコンテンツの再生を防止することが可能となる。

また、さらに、安全性を高めるため、コンテンツのインテグリティ・チェック値 (ICV) を書き換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわち $ICV = hash(Kicv, counter + 1, C1, C2, \dots)$ によって計算する構成とする。ここで、カウンタ $(counter + 1)$ は、 ICV の書き換え毎に 1 つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

さらに、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツと同一メディアに格納することができない構成においては、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツとは別のメディア上に格納する構成としてもよい。

例えば、読込専用メディアや通常の MO 等のコピー防止策のとられていないメディアにコンテンツを格納する場合、同一メディアにインテグリティ・チェック値 (ICV) を格納すると ICV の書換が不正なユーザによりなされる可能性が

あり、ICVの安全性が保てないおそれがある。このような場合、ホストマシン上の安全なメディアにICVを格納して、コンテンツのコピーコントロール（例えばcheck-in/check-out、move）にICVを使用する構成とすることにより、ICVの安全な管理及びコンテンツの改竄チェックが可能となる。

この構成例を図22に示す。図22では読込専用メディアや通常のMO等のコピー防止策のとられていないメディア2201にコンテンツが格納され、これらのコンテンツに関するインテグリティ・チェック値（ICV）を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア2202に格納し、ユーザによる不正なインテグリティ・チェック値（ICV）の書換を防止した例である。このような構成として、例えばメディア2201を装着したデバイスがメディア2201の再生を実行する際にホストマシンであるPC、サーバにおいてICVのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーコンテンツあるいは改竄コンテンツの再生を防止できる。

〔階層ツリー構造のカテゴリ分類〕

暗号鍵をルートキー、ノードキー、リーフキー等、図3の階層ツリー構造として構成し、コンテンツキー、認証キー、ICV生成キー、あるいはプログラムコード、データ等を有効化キーブロック（EKB）とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

図23に階層ツリー構造のカテゴリの分類の一例を示す。図23において、階層ツリー構造の最上段には、ルートキーKroot2301が設定され、以下の中間段にはノードキー2302が設定され、最下段には、リーフキー2303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

ここで、一例として最上段から第M段目のあるノードをカテゴリノード2304として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノード及びリーフと

する。

例えば図 2 3 の第 M 段目の 1 つのノード 2 3 0 5 にはカテゴリ [メモリスティック (商標)] が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノード又はリーフとして設定される。すなわち、ノード 2 3 0 5 以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、及びリーフの集合として定義する。

さらに、M 段から数段分下位の段をサブカテゴリノード 2 3 0 6 として設定することができる。例えば図 2 3 に示すようにカテゴリ [メモリスティック] ノード 2 3 0 5 の 2 段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器] のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード 2 3 0 6 以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード 2 3 0 7 が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる [P H S] ノード 2 3 0 8 と [携帯電話] ノード 2 3 0 9 を設定することができる。

さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば 1 つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器 X Y Z 専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器 X Y Z にその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック (E K B) を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

このように、1 つのノードを頂点としして、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の 1 つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キー

ブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

以上、説明したように、本発明の情報処理システム及び方法によれば、ツリー（木）構造の鍵配布構成により、コンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等の有効化キーブロック（EKB）とともに送信する構成としたので、正当なデバイスにおいてのみ復号可能な暗号データ配信が可能となるとともに配信メッセージ量を小さく押さえることができる。

また、ツリー構造の暗号化キー、データ配信方式を用いてコンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等を有効化キーブロック（EKB）とともに送信する構成において、さらに、共通鍵方式、あるいは公開鍵方式の認証処理を併用する構成とすれば、さらに安全なデータ配信が可能となる。

また、本発明の情報処理システム及び方法によれば、コンテンツに対するインテグリティ・チェック値（ICV）をコンテンツを格納した記録媒体、あるいはその他のメディアに格納してコンテンツ改竄のチェック、あるいはコピーチェックを可能としたので、不正なコンテンツの流通を防止することが可能になる。

また、本発明の情報処理システム及び方法によれば、ツリー構造の暗号化キー、データ配信方式において、階層ツリーをカテゴリ毎に分類して、各カテゴリの管理する頂点ノード以下のノード、リーフを特定のデバイスに限定する構成としたので、各カテゴリの管理者が独自に有効化キーブロック（EKB）を生成して管

理下にあるデバイスに対して配信することが可能になる。

請求の範囲

1. 1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、

個々のデバイスは、

複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、

前記暗号化メッセージデータを配信するメッセージデータ配信手段は、

前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいづれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成して配信する構成を有することを特徴とする情報処理システム。

2. 前記デバイスにおける前記暗号処理手段は、前記有効化キーブロック（EKB）の処理により、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする請求の範囲第1項に記載の情報処理システム。

3. 前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求の範囲第1項に記載の情報処理システム。

4. 前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第1項に記載の情報処理システム。

5. 前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求の範囲第1項に記載の情報処理システム。

6. 前記メッセージデータは、プログラムコードであることを特徴とする請求の

範囲第 1 項に記載の情報処理システム。

7. 前記メッセージデータ配信手段は、前記有効化キーブロック (E K B) と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと、前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信する構成であることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

8. 前記メッセージデータ配信手段と前記デバイスは、それぞれ認証処理を実行する認証処理手段を有し、

前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信する構成であることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

9. 前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、

前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック (E K B) と暗号化メッセージデータを生成して配信する構成を有することを特徴とする請求の範囲第 1 項に記載の情報処理システム。

10. 前記階層ツリー構造は、1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループによって構成されるカテゴリグループを含み、

該カテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたカテゴリに属するデバイスの集合として構成されていることを特徴とする請求の範囲第 1 項に記載の情報処理システム。

11. 前記カテゴリグループは、さらに前記階層ツリー構造の下位段に 1 以上のサブカテゴリを含み、

該サブカテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたサブカテゴリに属するデバイスの集合として構成されていることを特徴とする請求の範囲第 10 項に記載の情報処理システム。

12. 1 以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデ

ータをメッセージデータ配線手段から配信する情報処理方法であり、

複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック (E K B) を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、

前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップとを有する情報処理方法。

13. 前記復号処理ステップは、

前記有効化キーブロック (E K B) の処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含むことを特徴とする請求の範囲第12項に記載の情報処理方法。

14. 前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求の範囲第12項に記載の情報処理方法。

15. 前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第12項に記載の情報処理方法。

16. 前記メッセージデータは、コンテンツのインテグリティ・チェック値 (I C V) 生成キーであることを特徴とする請求の範囲第12項に記載の情報処理方法。

17. 前記メッセージデータは、プログラムコードであることを特徴とする請求の範囲第12項に記載の情報処理方法。

18. 前記メッセージデータ配信手段は、前記有効化キーブロック (E K B) と、

前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする請求の範囲第 1 2 項に記載の情報処理方法。

19. 前記メッセージデータ配信手段と前記デバイスは、相互間の認証処理を実行し、

前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信することを特徴とする請求の範囲第 1 2 項に記載の情報処理方法。

20. 前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、

前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キープブロック (EKB) と暗号化メッセージデータを生成して配信することを特徴とする請求の範囲第 1 2 項に記載の情報処理方法。

21. データを格納した情報記録媒体であり、

複数の異なるデバイスをリーフとした階層ツリー構造の 1 つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープブロック (EKB) と、

前記更新ノードキーによって暗号化したメッセージデータとを格納したことを特徴とする情報記録媒体。

22. 前記メッセージデータは、コンテンツの復号に用いるコンテンツキーであり、

前記情報記録媒体は、さらに、前記コンテンツキーによって暗号化された暗号化コンテンツを格納した構成であることを特徴とする請求の範囲第 2 1 項に記載の情報記録媒体。

23. 前記情報記録媒体は、さらに、コンテンツと該コンテンツの対応するコン

テンツキーを取得するために使用される有効化キープロック (EKB) を対応付けた対応付けデータを格納していることを特徴とする請求の範囲第 22 項に記載の情報記録媒体。

24. 前記情報記録媒体は、さらに、コンテンツのインテグリティ・チェック値 (ICV) データを格納していることを特徴とする請求の範囲第 21 項に記載の情報記録媒体。

25. 暗号化コンテンツデータの復号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、

前記コンピュータ・プログラムは

複数の異なるデバイスをリーフとした階層ツリー構造の 1 つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーに対して、該グループのノードキーあるいはリーフキーによって暗号化した有効化キープロック (EKB) の復号処理により、更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するステップと、

前記コンテンツキーにより前記暗号化コンテンツの復号を実行するステップとを含むことを特徴とするプログラム提供媒体。

26. 1 以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理方法であって、

複数の異なるデバイスをリーフとした階層ツリー構造の 1 つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープロック (EKB) とを生成し、

前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するようになすことを特徴とする情報処理方法。

27. 上記メッセージデータは、コンテンツデータを復号するための復号鍵とし

て使用可能なコンテンツキーであることを特徴とする請求の範囲第26項に記載の情報処理方法。

28. 上記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第26項に記載の情報処理方法。

29. 上記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求の範囲第26項に記載の情報処理方法。

30. 前記有効化キーブロック（EKB）と、

前記メッセージデータとしてコンテンツデータを復号する為の復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする請求の範囲第26項に記載の情報処理方法。

31. 複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーに対して、該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）の復号処理を行うことにより、上記更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するコンテンツキー取得ステップと、

前記コンテンツキーにより前記暗号化コンテンツの復号を実行する実行ステップとを含むことを特徴とする情報処理方法。

[2001年7月27日(27.07.01)国際事務局受理:新しい請求の範囲32及び33が加えられた;他の請求の範囲は変更なし。(3頁)]

て使用可能なコンテンツキーであることを特徴とする請求の範囲第26項に記載の情報処理方法。

28. 上記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求の範囲第26項に記載の情報処理方法。

29. 上記メッセージデータは、コンテンツのインテグリティ・チェック値(ICV)生成キーであることを特徴とする請求の範囲第26項に記載の情報処理方法。

30. 前記有効化キーブロック(EKB)と、

前記メッセージデータとしてコンテンツデータを復号する為の復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする請求の範囲第26項に記載の情報処理方法。

31. 複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーに対して、該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック(EKB)の復号処理を行うことにより、上記更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するコンテンツキー取得ステップと、

前記コンテンツキーにより前記暗号化コンテンツの復号を実行する実行ステップとを含むことを特徴とする情報処理方法。

32. (追加) 1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、

個々のデバイスは、

複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、

前記暗号化メッセージデータを配信するメッセージデータ配信手段は、

前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープロック（EKB）を生成するとともに、前記更新ノードキーによって暗号化した暗号化メッセージデータを生成して配信する構成を有し、

前記メッセージデータ配信手段は、

前記更新ノードキーを利用して暗号化した暗号化メッセージデータと、

前記選択されたデバイス以外のデバイスが保有していないリーフキー、あるいはノードキーを利用して暗号化された前記更新ノードキーを1つ以上含む有効化キープロック（EKB）とを生成すると共に、上記暗号化メッセージデータと上記有効化キープロックとを共に配信し、

前記選択されたデバイスは、

前記選択されたデバイスのみが保有している前記キーセット及び前記有効化キープロックを利用して前記暗号化メッセージデータを元のメッセージデータに復号するようになすことを特徴とする情報処理システム。

33.（追加）複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットがそれぞれ規定されており、そのうちの1つを保有するキーセット記憶手段と、

前記キーセット記憶手段に記憶されている前記ノードキー及び前記リーフキーあるいは配信されるキーを用いることにより、暗号化データを復号化する暗号処理手段を有し、

前記暗号処理手段は、

前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノード及びリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーによって暗号化したメッセージデータと、

選択されたデバイス以外のデバイスが保有していないリーフキー、あるいはノ

ードキーを利用して暗号化された前記更新ノードキーを1つ以上含む有効化キーブロック（EKB）とを含む暗号化データに対して、前記キーセット記憶手段に保有されているリーフキーあるいはノードキーによって前記メッセージデータを暗号化した更新ノードキーを復号化し、

該更新ノードキーで前記暗号化メッセージデータを復号化するようになすことを特徴とする情報処理装置。

1/23

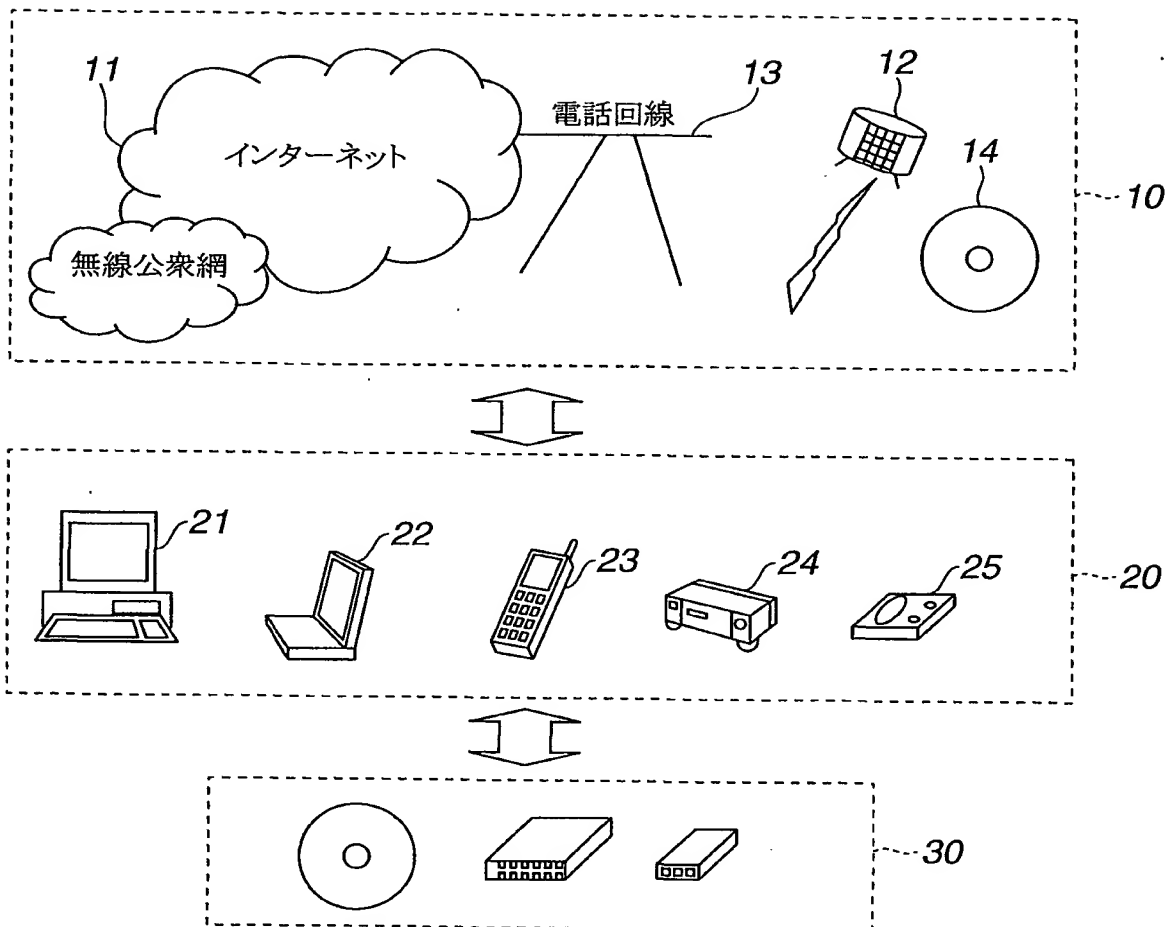


FIG. 1

2/23

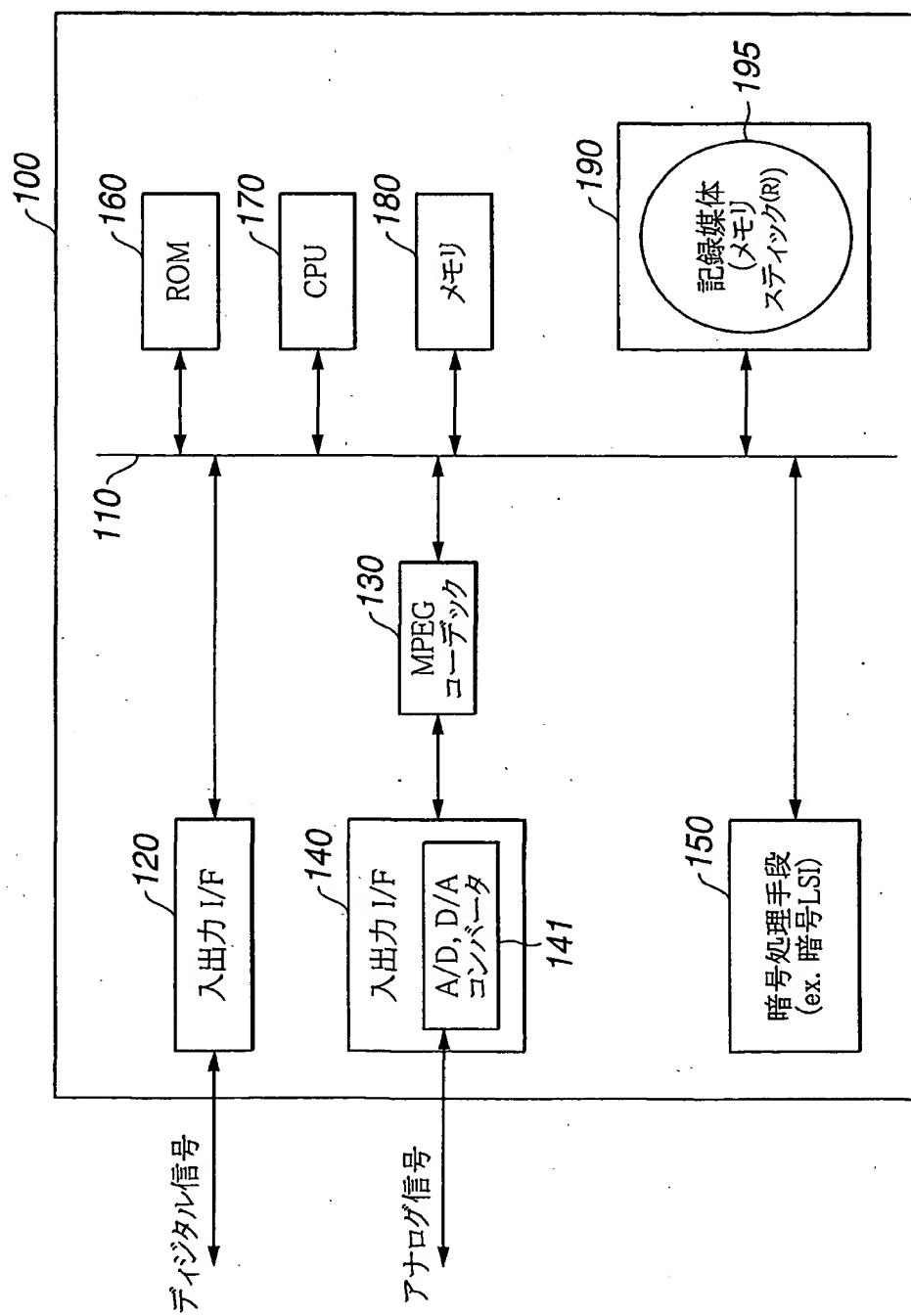


FIG.2

3/23

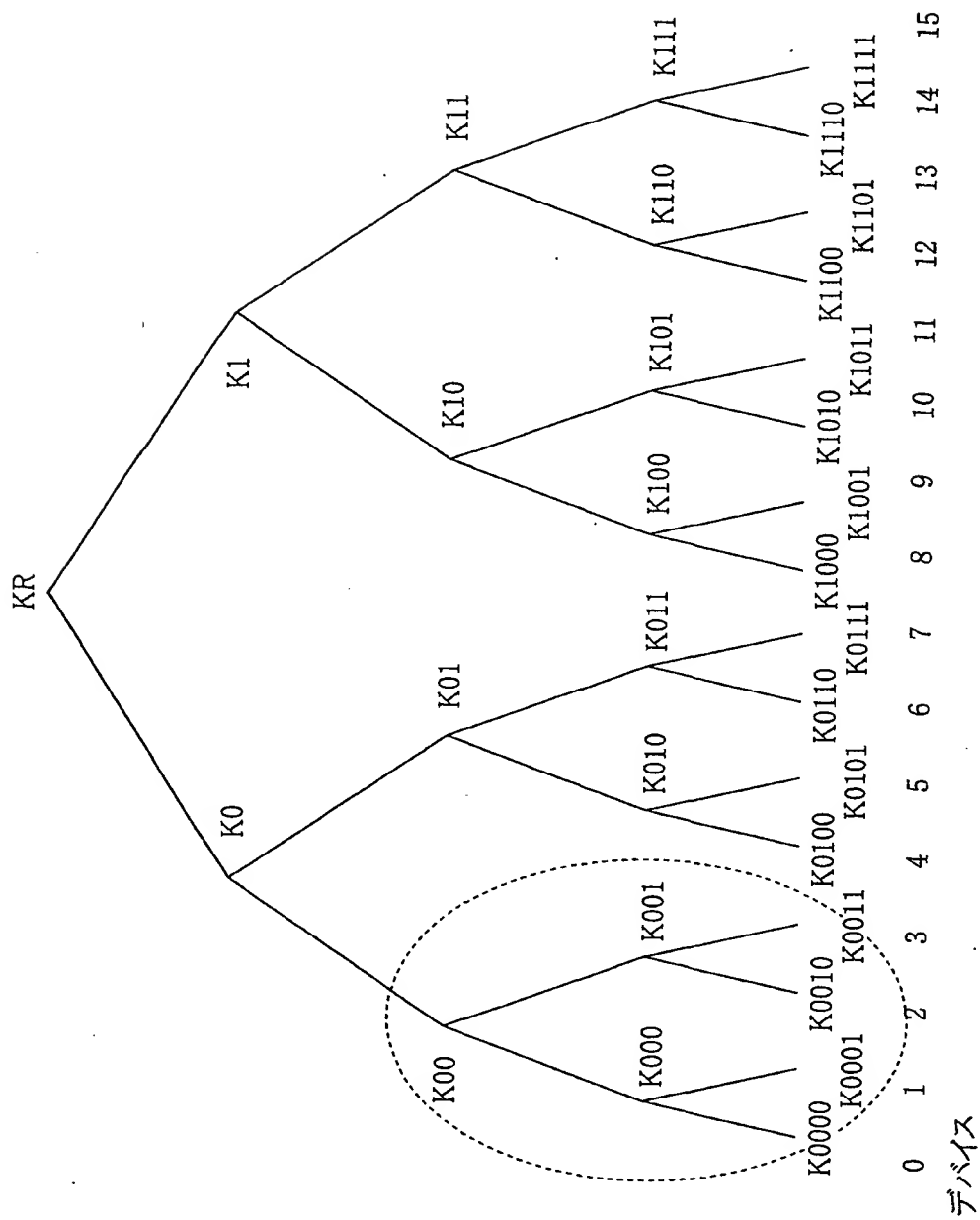


FIG.3

4/23

バージョン (Version) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.4A

バージョン (Version) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.4B

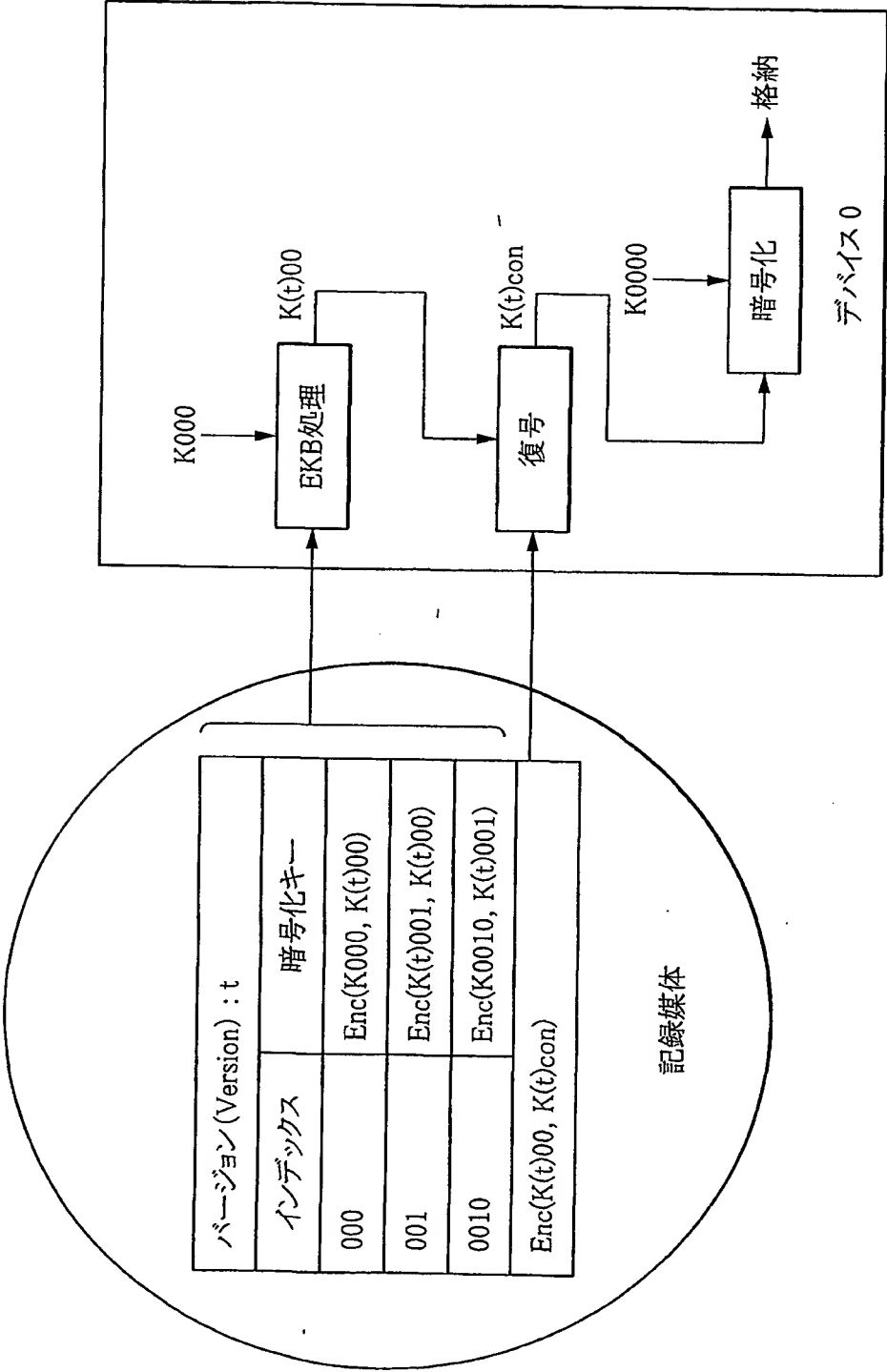


FIG.5

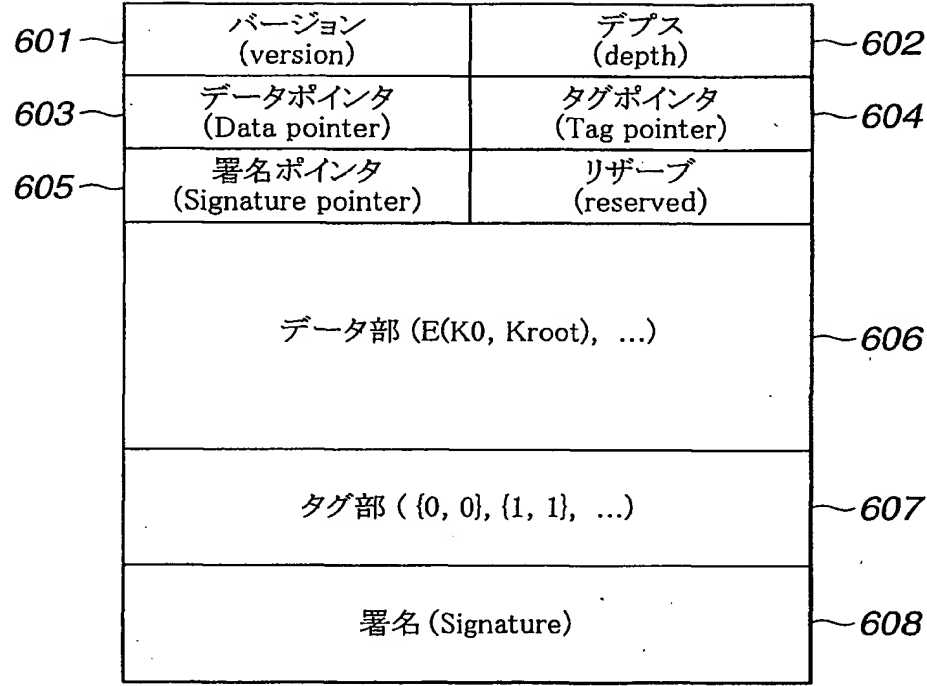


FIG.6

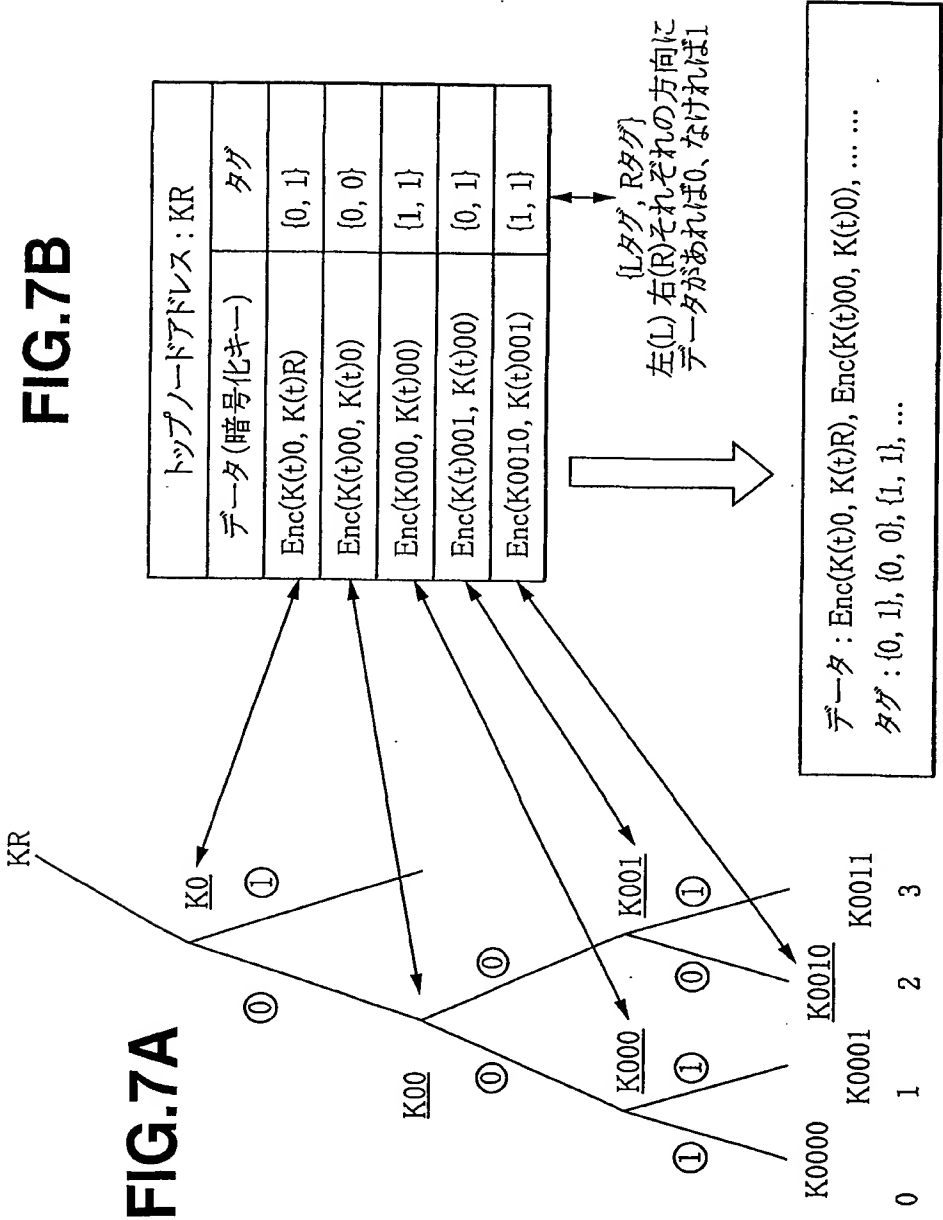


FIG.8A

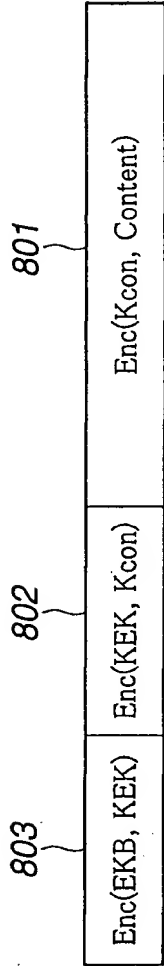
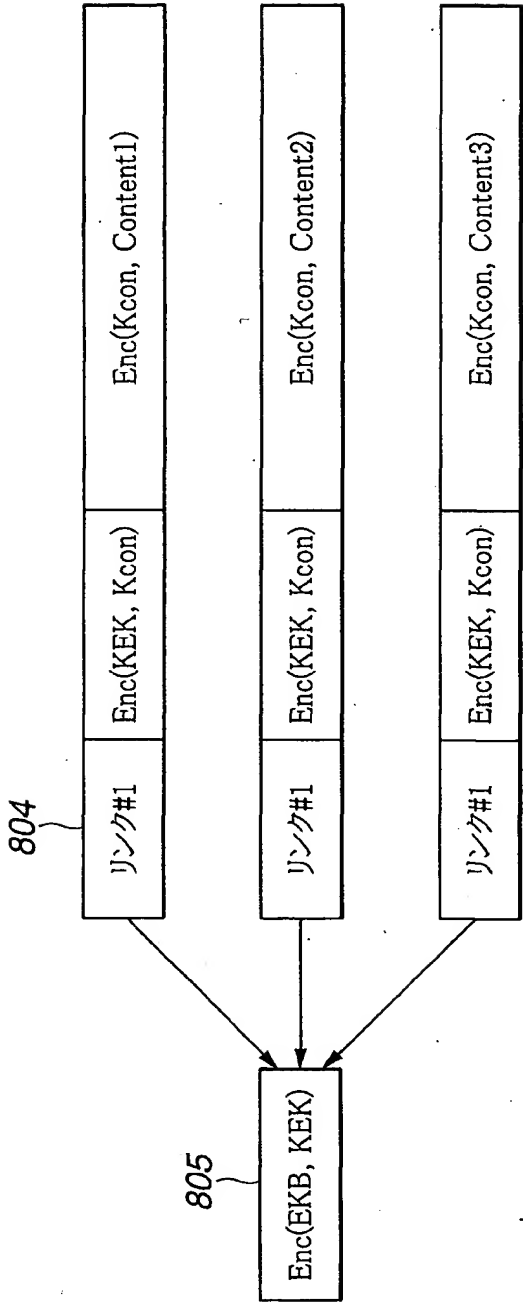


FIG.8B



9/23

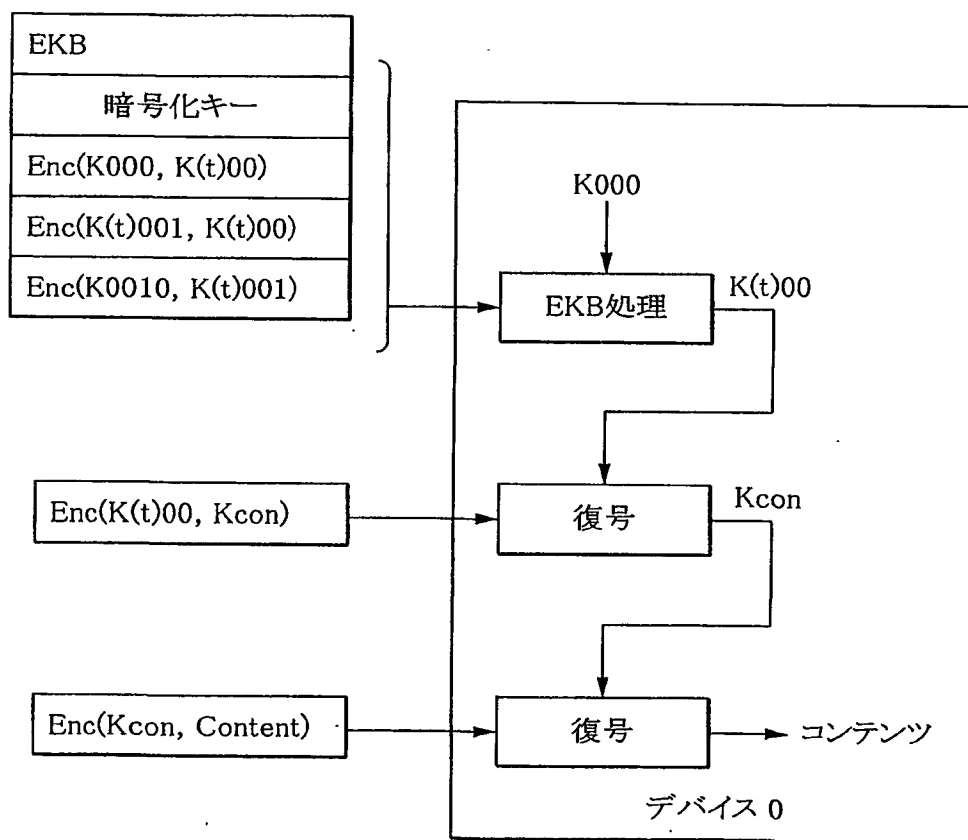


FIG.9

10/23

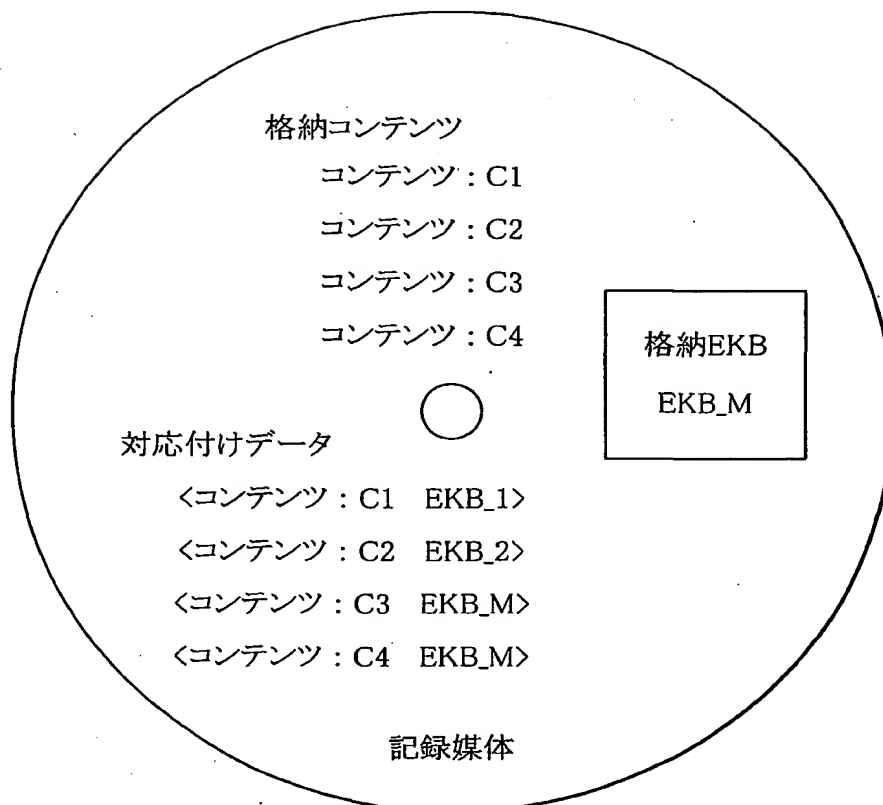


FIG.10

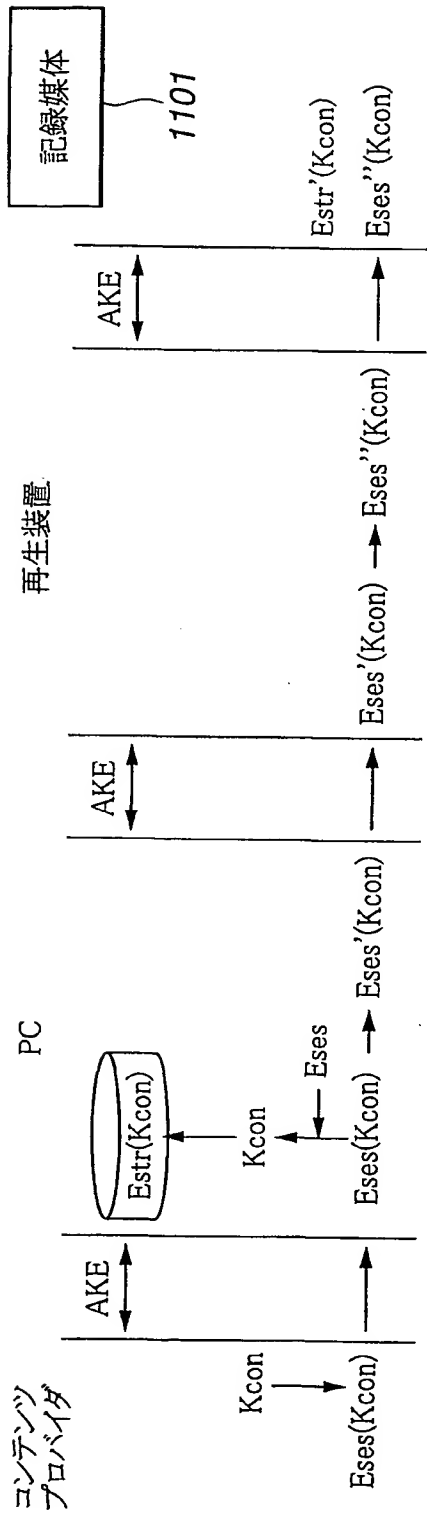


FIG.11A

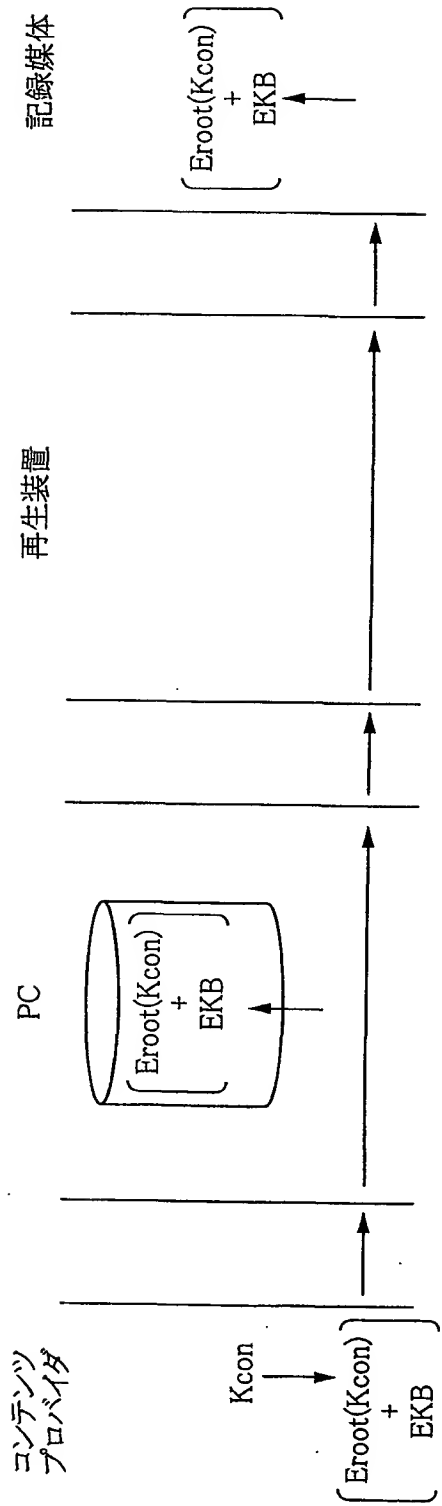


FIG.11B

12/23

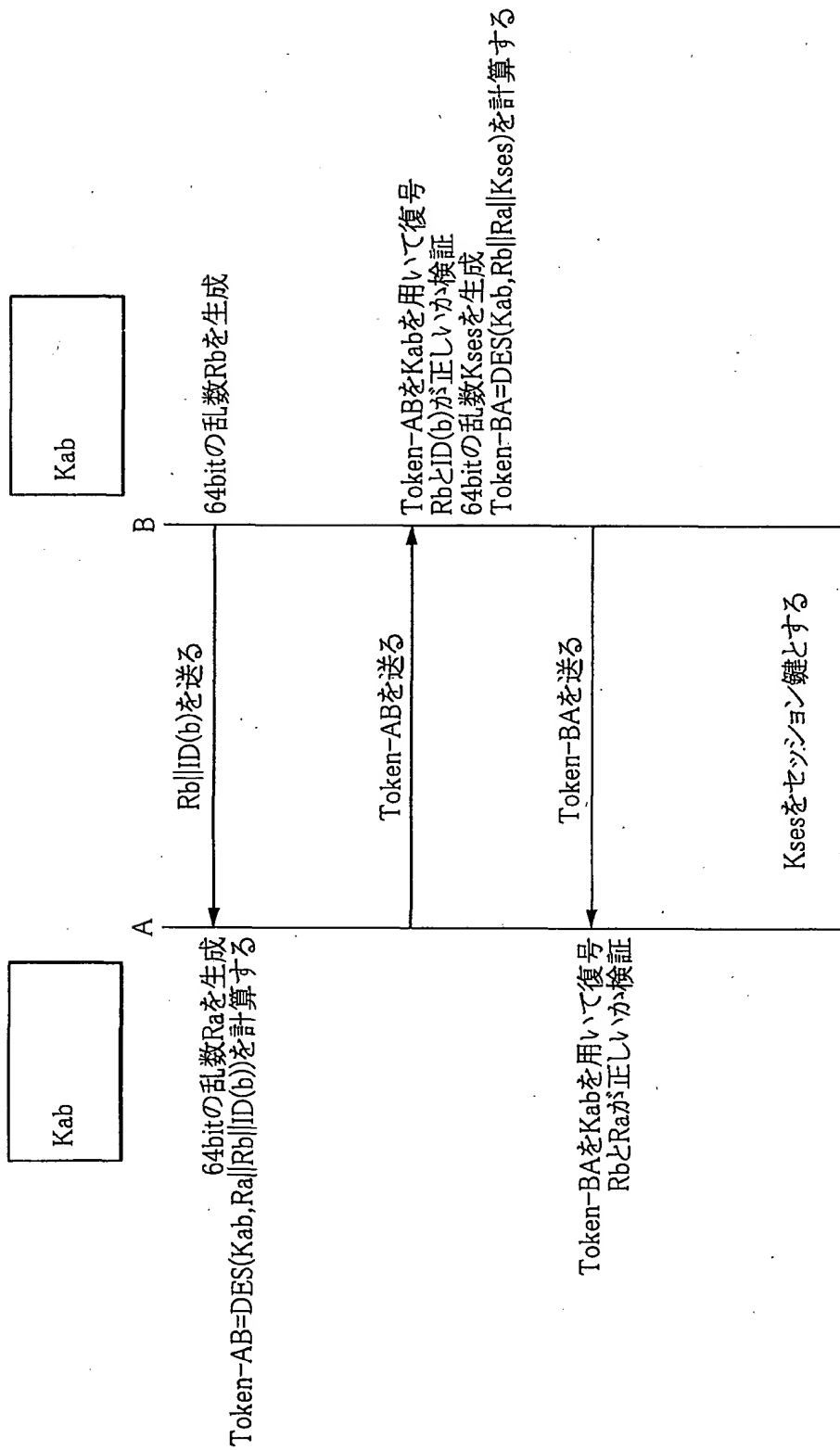


FIG.12

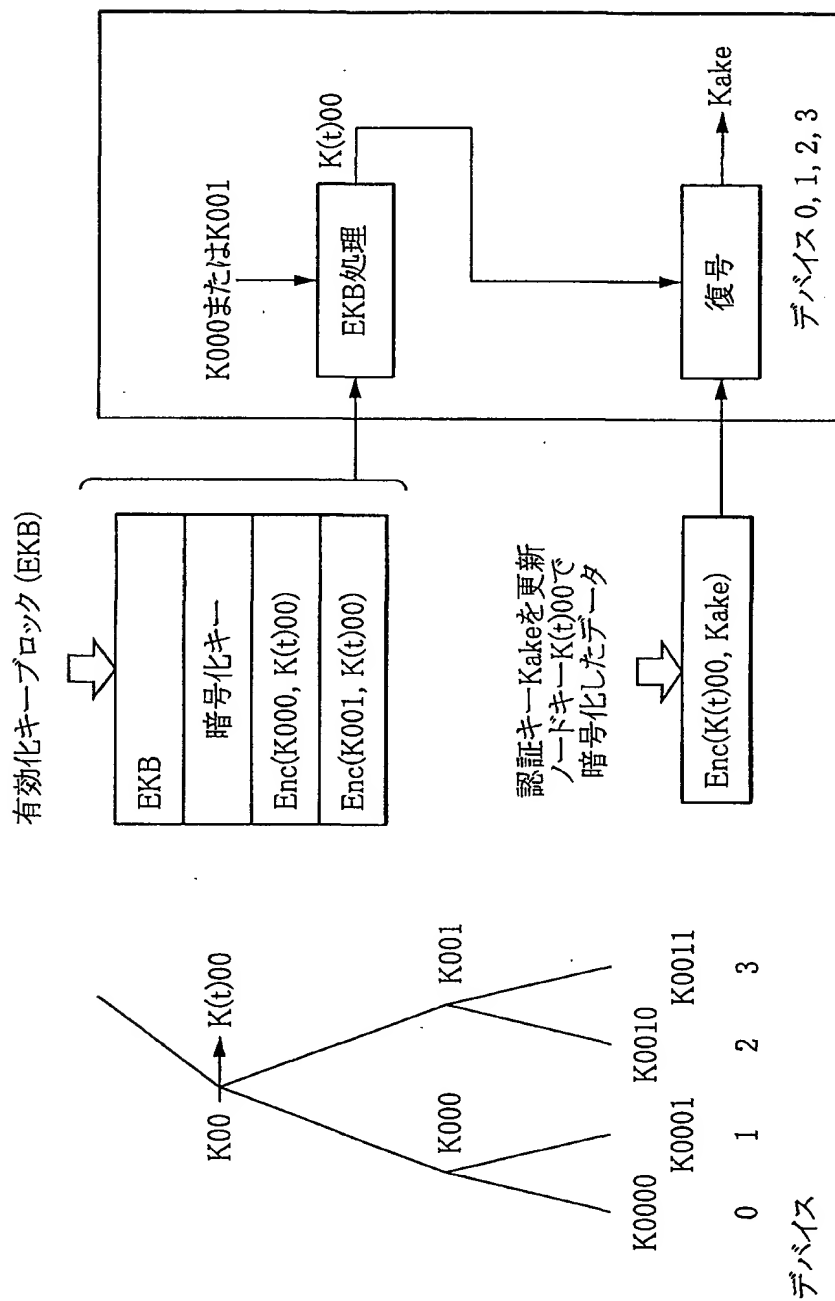


FIG.13

14/23

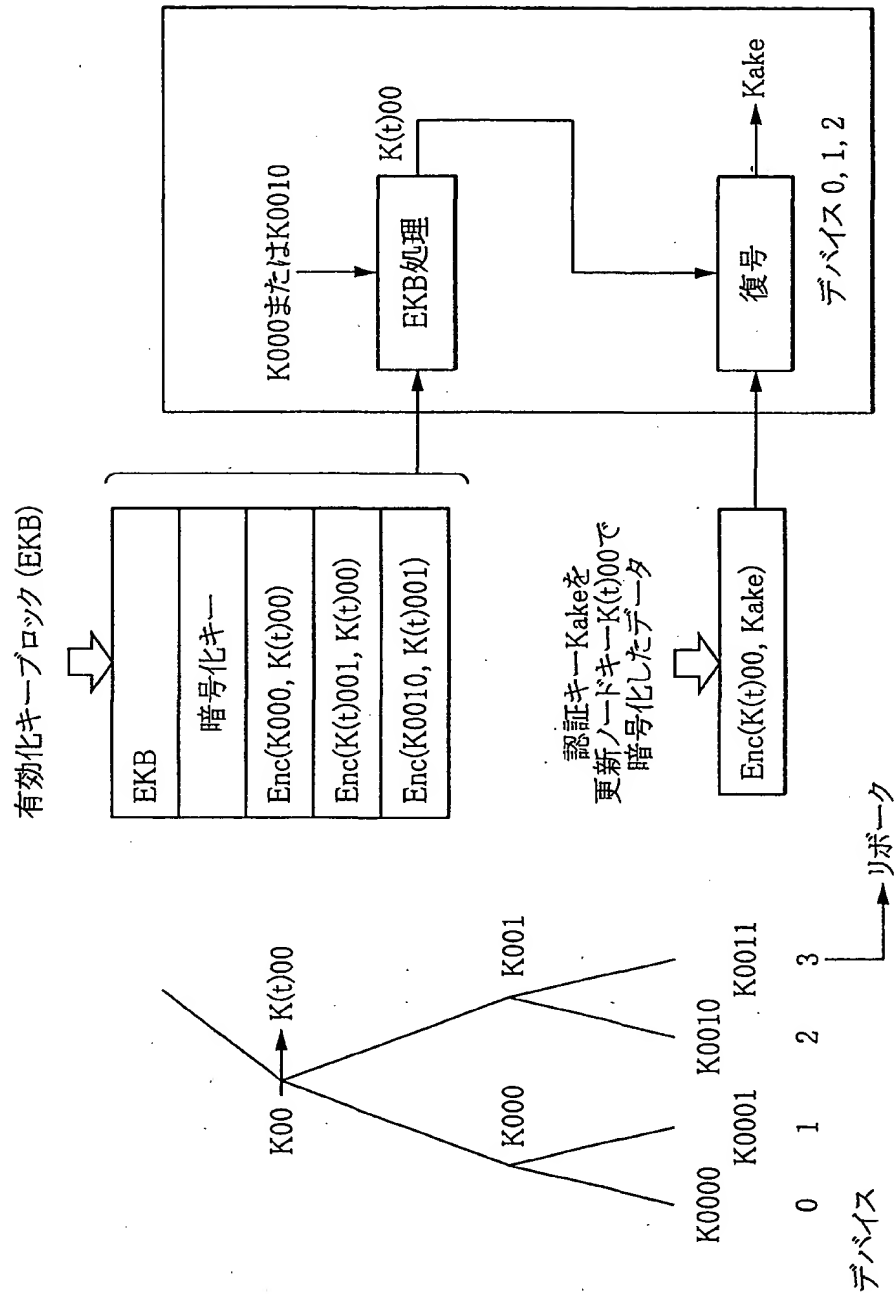


FIG.14

15/23

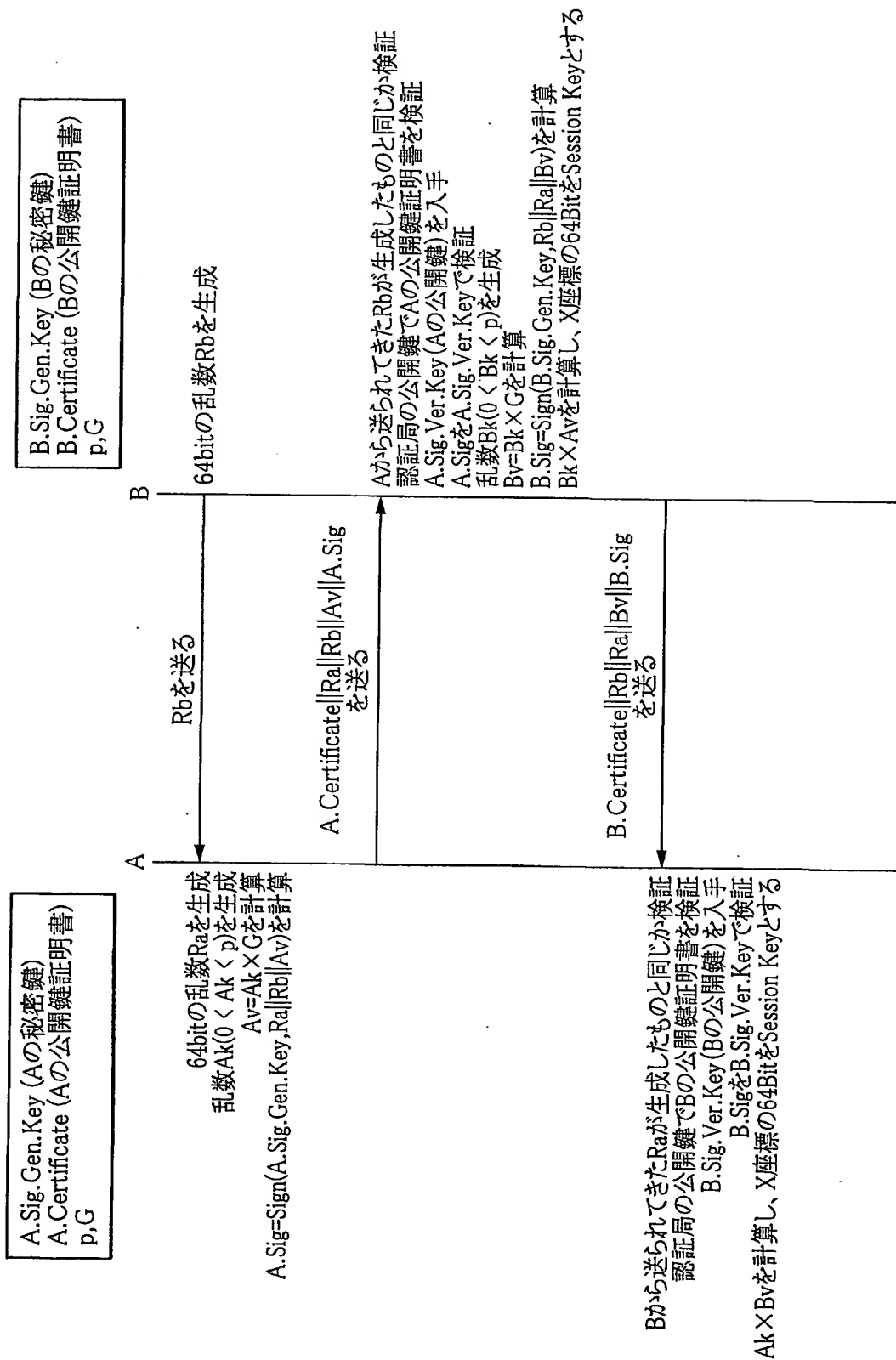


FIG.15

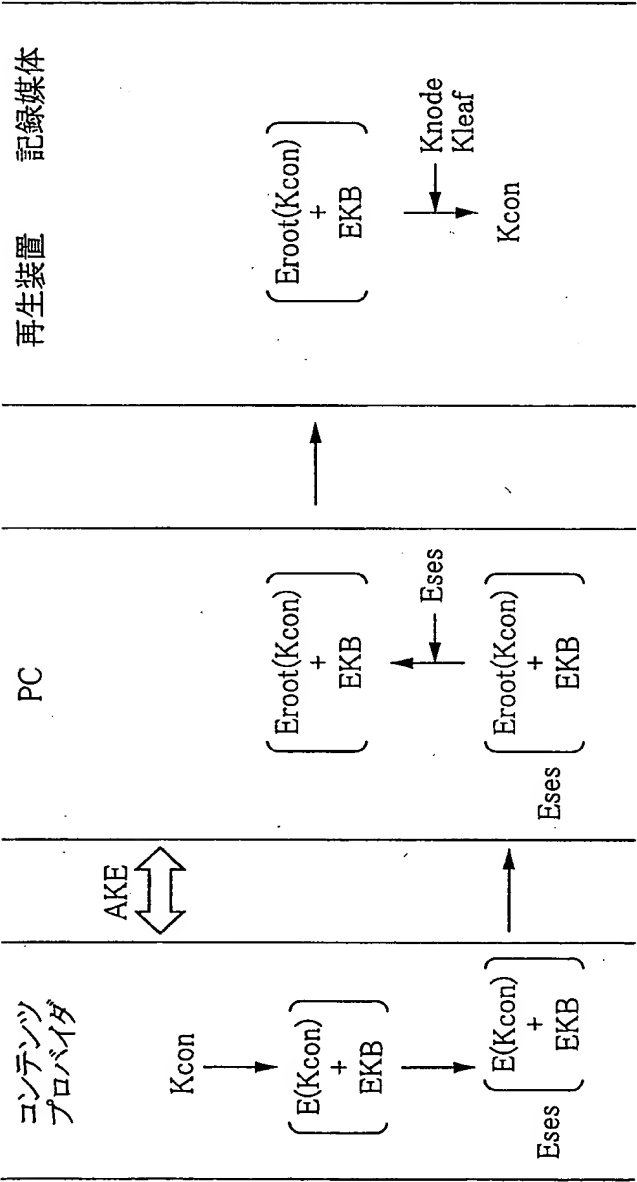


FIG.16

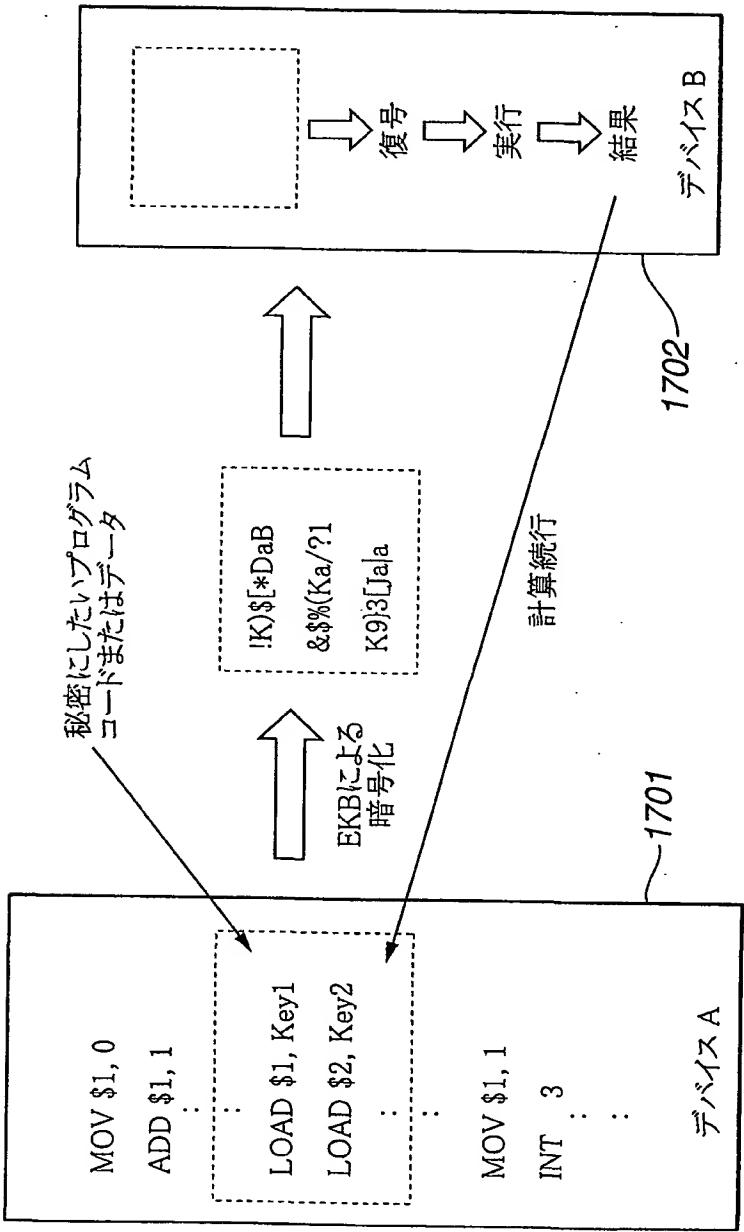
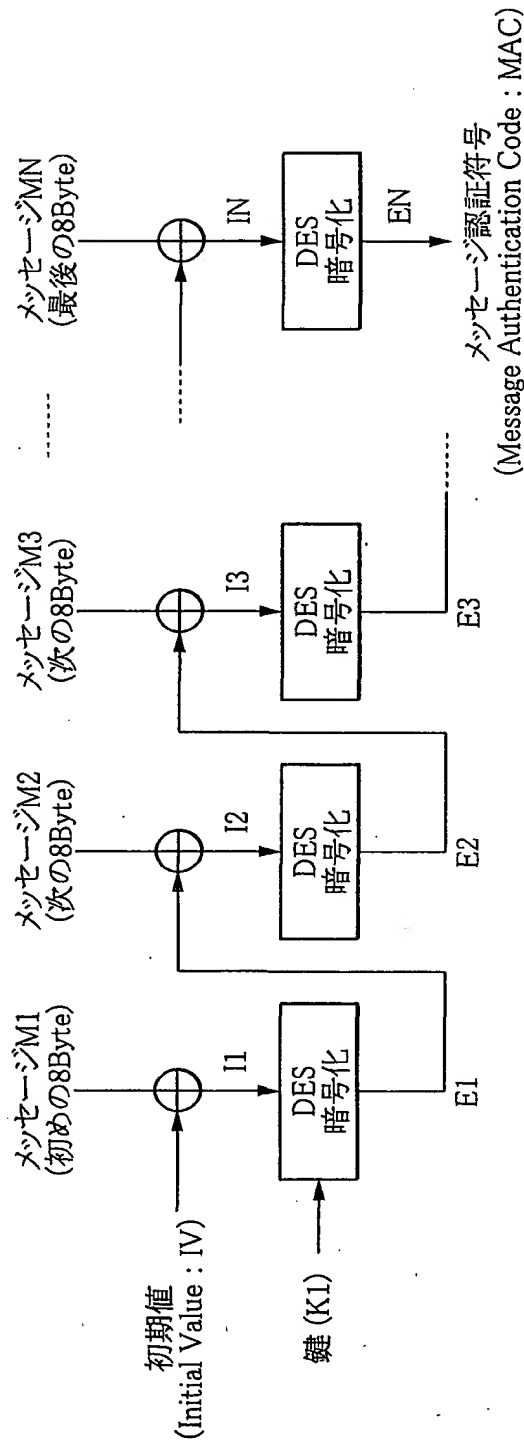


FIG.17



⊕ : 排他的論理和処理 (8バイト単位)

FIG.18

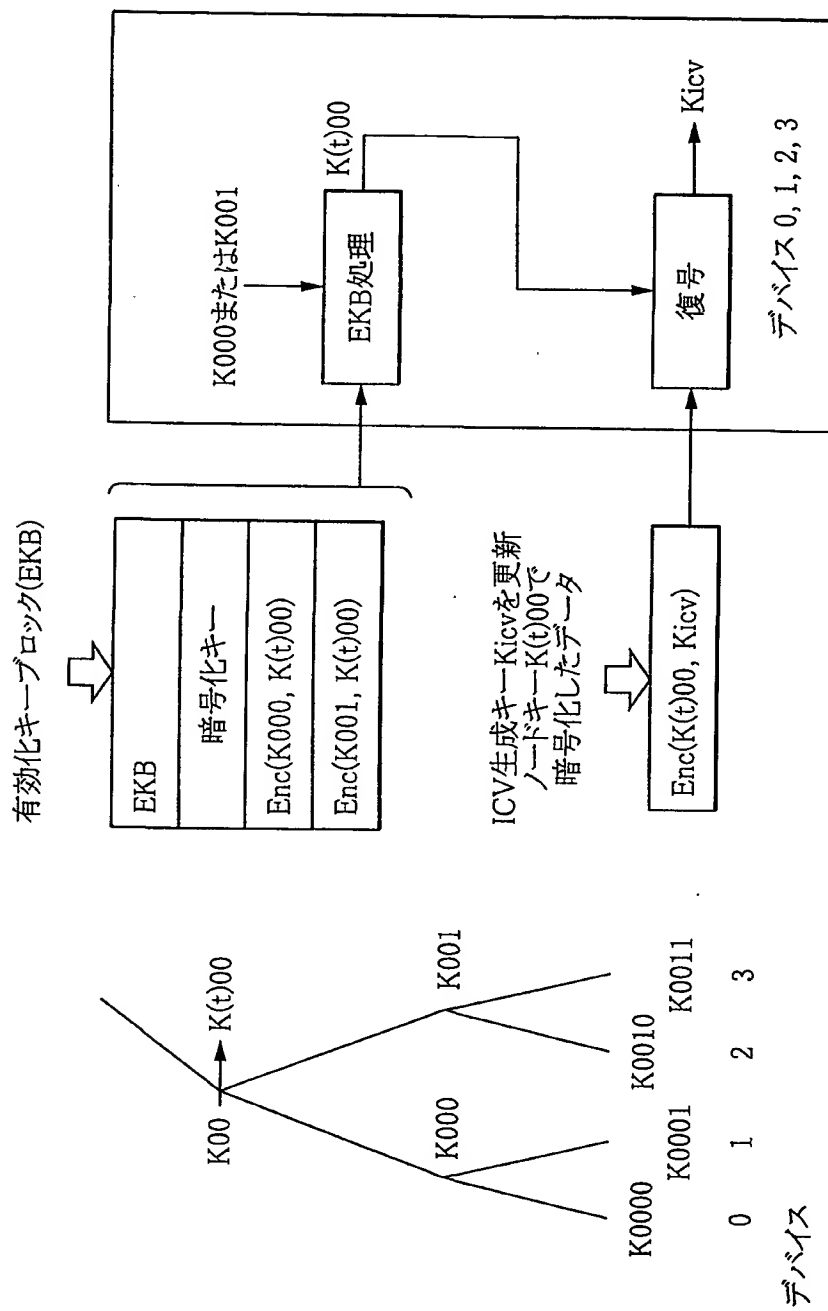


FIG. 19

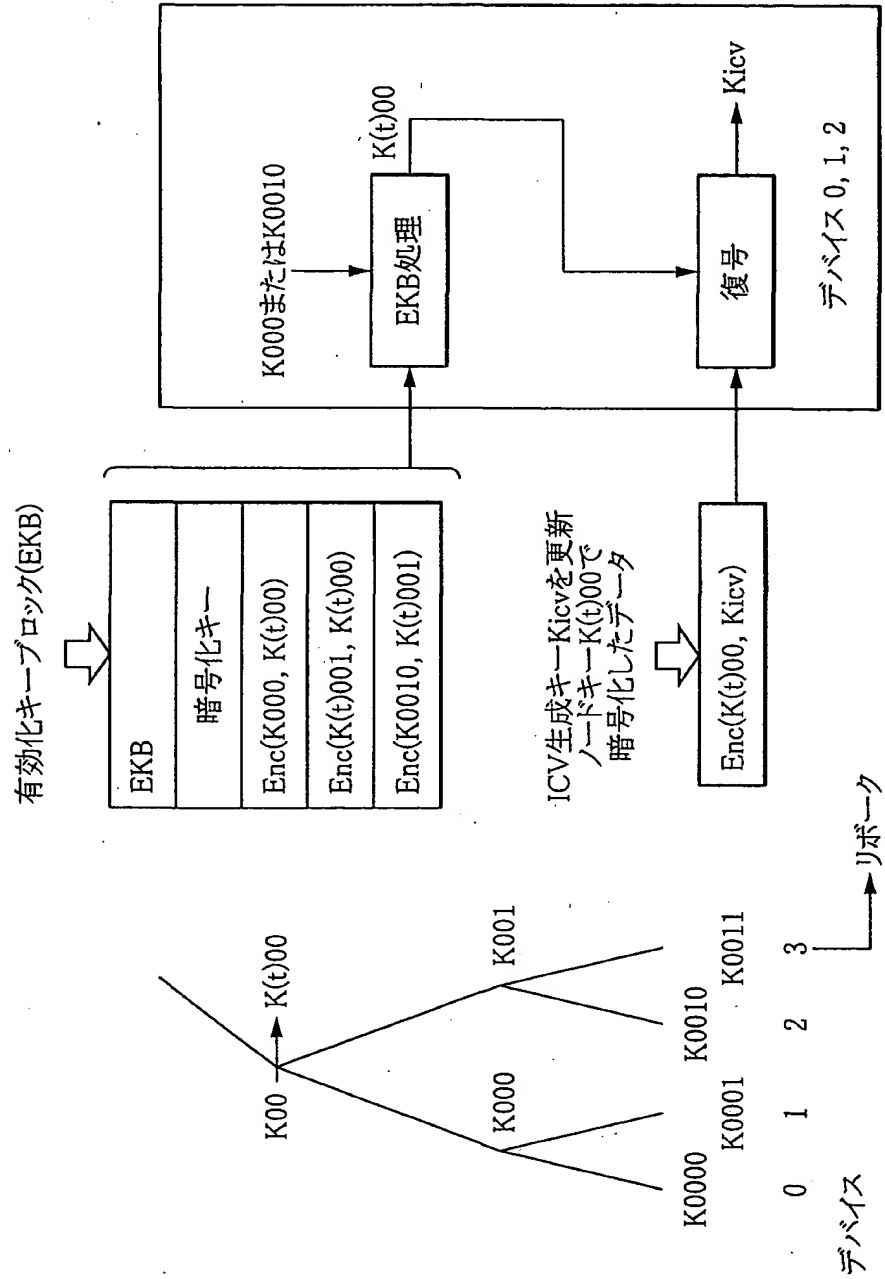


FIG.20

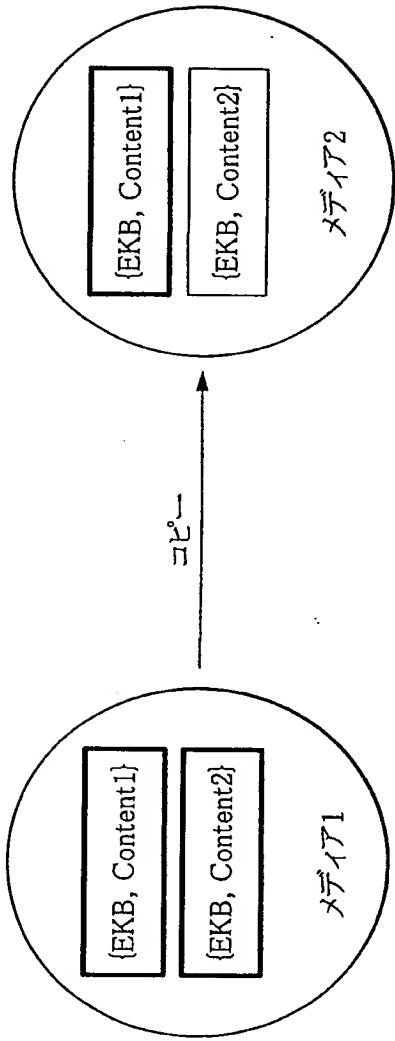


FIG.21A

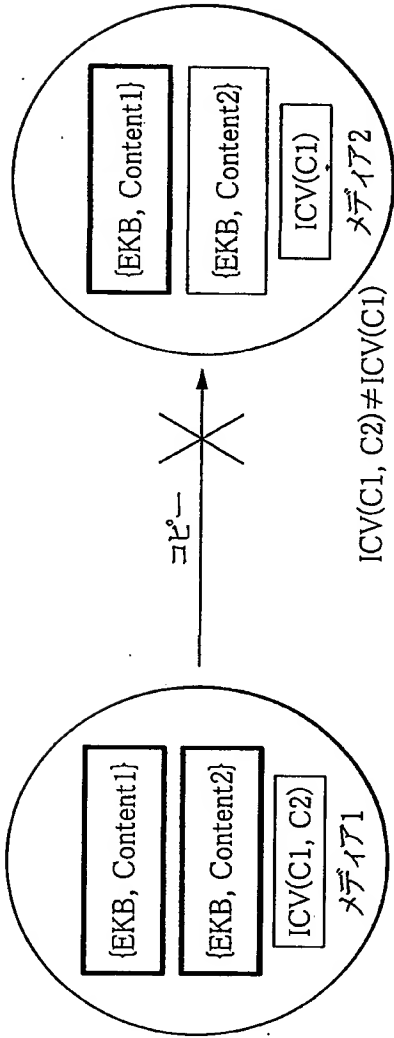


FIG.21B

22/23

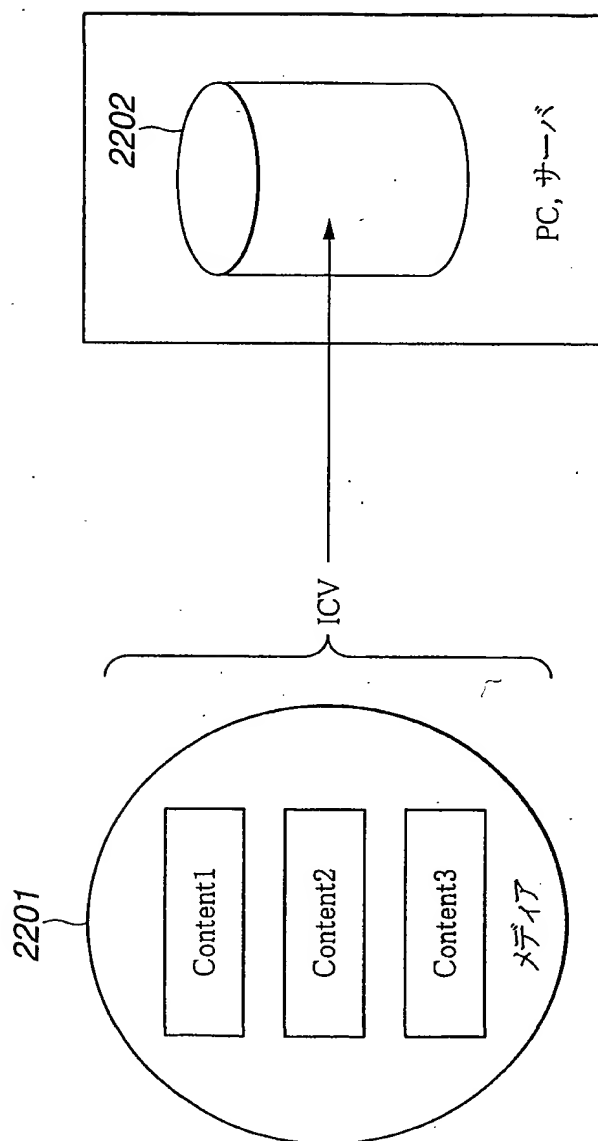


FIG.22

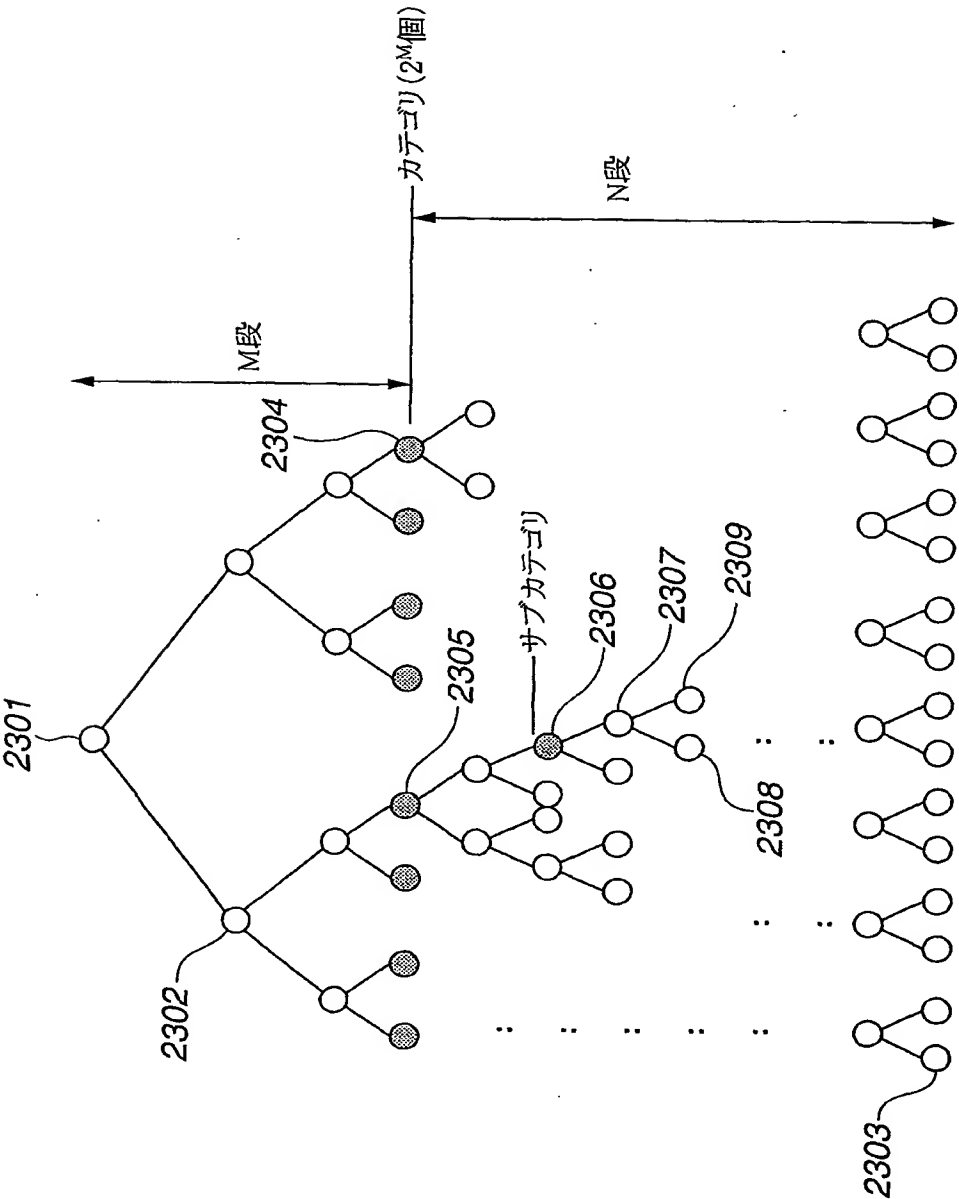


FIG.23

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02866

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST DATABASE on Science and Technology key, tree

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 11-187013, A (IBM Japan, Ltd.), 09 July, 1999 (09.07.99),	1-21, 25-31
Y	Par. Nos. 9 to 11, 17 to 22 & CN, 1224962, A	22-24
X	"The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications,	1-20, 25-31
Y	Vol.17, No.9, pp.1614-1631 September, 1999 (09.99), Page 1616, right column to page 1621, left column	21-24
X	"Secure Group Communications Using Key Graphs", Proceedings of ACM SIGCOMM'98, p.68-79	1-20, 25-31
Y	02 September, 1998 (02.09.98), 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	21-24
Y	JP, 11-250568, A (Sony Corporation), 17 September, 1999 (17.09.99), Par. Nos. 2 to 5 (Family: none)	21-24

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not
considered to be of particular relevance
"E" earlier document but published on or after the international filing
date
"I" document which may throw doubts on priority claim(s) or which is
cited to establish the publication date of another citation or other
special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other
means
"P" document published prior to the international filing date but later
than the priority date claimed

"T" later document published after the international filing date or
priority date and not in conflict with the application but cited to
understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be
considered novel or cannot be considered to involve an inventive
step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be
considered to involve an inventive step when the document is
combined with one or more other such documents, such
combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
16 May, 2001 (16.05.01)

Date of mailing of the international search report
22 May, 2001 (22.05.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02866

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
EX	US, 6049878, A (Sun Microsystems, Inc.), 11 April, 2000 (11.04.00), Full text (Family: none)	1-20, 25-31
A	US, 5748736, A (S, Mittra), 05 May, 1998 (05.05.98), Full text (Family: none)	1-31
EA	WO, 01/03364, A1 (Matsushita Electric Ind. Co., LTD.), 11 January, 2001 (11.01.01), Full text (Family: none)	1-31
EA	WO, 01/03365, A1 (Matsushita Electric Ind. Co., LTD.), 11 January, 2001 (11.01.01), Full text (Family: none)	1-31

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G06F17/60, G11B20/10, G11B20/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST 科学技術文献データベース key, tree

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 11-187013, A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落	1-21, 25-31
Y	& CN, 1224962, A	22-24
X	"The VersaKey Framework:Versatile Group Key Management", IEEE Journal on Selected Areas in Communications,	1-20, 25-31
Y	Vol. 17, No. 9, p. 1614-1631 9月.1999(09.99) 第1616頁右欄-第1621頁左欄	21-24
X	"Secure Group Communications Using Key Graphs", Proceedings of ACM SIGCOMM' 98, p. 68-79	1-20, 25-31
Y	2. 9月.1998(02.09.98) 3.4 Leaving a tree key graph	21-24

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

16.05.01

国際調査報告の発送日

22.05.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正



5M

9364

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	(http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	
Y	JP, 11-250568, A (ソニー株式会社) 17. 9月. 1999 (17. 09. 99) 第2-5段落 (ファミリー無し)	21-24
EX	US, 6049878, A (Sun Microsystems, Inc.) 11. 4月. 2000 (11. 04. 00) 全頁を参照 (ファミリー無し)	1-20, 25-31
A	US, 5748736, A (S. Mittra) 5. 5月. 1998 (05. 05. 98) 全頁を参照 (ファミリー無し)	1-31
EA	WO, 01/03364, A1 (Matsushita Electric Industrial Co., LTD.) 11. 1月. 2001 (11. 01. 01) 全頁を参照 (ファミリー無し)	1-31
EA	WO, 01/03365, A1 (Matsushita Electric Industrial Co., LTD.) 11. 1月. 2001 (11. 01. 01) 全頁を参照 (ファミリー無し)	1-31